Aspera Faspex Admin Guide 3.5

Windows XP, 2003, 2008

Document Version: V1

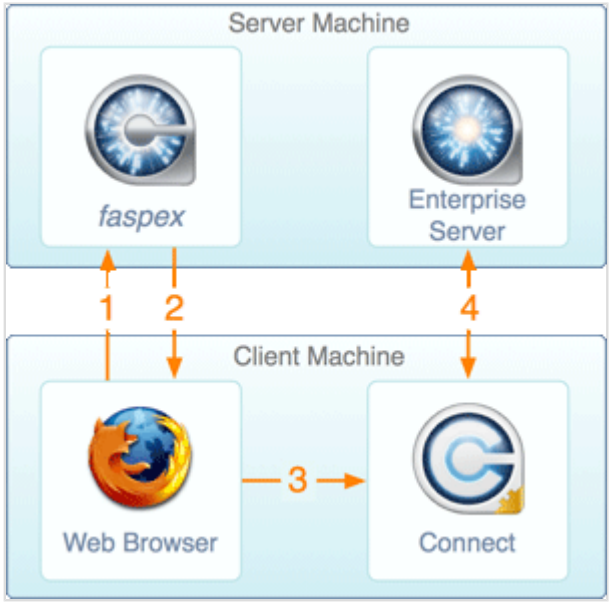
Contents

Introduction

Aspera Faspex Server is a file exchange application built upon Aspera Enterprise Server as a centralized transfer solution. With a web-based graphical user interface, Faspex Server offers more advanced management options for *fasp* high-speed transfer to match your organization's workflow. Faspex offers the following file-exchange and management features:

Feature	Description
Web/Email-based Interface	Simple web and email interface for exchanging files and directories.
Package Forwarding	Enable users to forward file packages on the server to others (without re-uploading).
Permission Management	Manage user permissions through workgroup/dropbox assignment or direct-configuration.
Post-Processing	Execute custom scripts after a transfer when certain conditions are met.
Email Notification	Create customizable email notifications of Faspex events (such as receiving a package).
Directory Service	Seamlessly integrate your organization’s Directory Service users and groups.

The following diagram illustrates how Faspex Server handles file transfers:



1. **End user accesses the Faspex website via a web browser. At this point, the Faspex Website triggers the Aspera Connect browser plugin. If the user has not already installed the browser plugin, the website will prompt the user automatically.**
2. **Faspex returns the server’s file list or an upload page based upon the end user’s request.**

3. **When the end user selects a file for download or upload, transfer information is passed to the Aspera Connect browser plugin.**
4. **The Aspera Connect browser plugin establishes a connection with Enterprise Server and begins transferring file(s).**

Installation

Prepare your system and install Aspera Faspex.

System Requirements

Prepare your system for Aspera Faspex.

System Requirements for Aspera Faspex 3.5:

- 4 GB RAM
- Windows XP, 2003, 2008
- Aspera Enterprise Server v3.0+.
- If your computer has an existing MySQL database installed, ensure that it is not running during the installation.
- If your computer has an existing Apache HTTP server installed, ensure that it is not running during the installation.
- If you are upgrading your existing Faspex Server, be sure to have your MySQL and svcAspera passwords accessible prior to the upgrade.

For firewall requirements, please refer to the topic *Configuring the Firewall* on page 18.

Faspex Upgrade Checklist

Prerequisites for attempting to upgrade to a newer version of Faspex.

IMPORTANT NOTE: If you are running your Aspera Enterprise Server on Isilon OneFS, do not upgrade to Faspex v3.0+! You should not upgrade until Aspera Enterprise Server 3.x is available on your Isilon OneFS platform .

If you are currently running...	Then, you must do the following to upgrade to Faspex v3.0+:
Faspex v2.6.5+	You can upgrade directly to 3.0+ by following the instructions in the topic "*Upgrade Procedure*."
Faspex v2.5.3	You can upgrade directly to 3.0+; however, you must install an updated license to upgrade (since the license format for Faspex v2.6.5+ has changed). To obtain the new, FREE license, please contact *Aspera Technical Support*. Once you have obtained your new license, you must copy it into the Faspex Server license directory and restart Faspex, as described in the topic *License* on page 64.
Faspex v2.0.8 or v2.0.10	You must first upgrade to 2.5.3 by following the *upgrade instructions* for this version. Please contact *Technical Support* on page 175 if you do not have the requisite installer.

If you are currently running...	Then, you must do the following to upgrade to Faspex v3.0+:
Faspex v1.6 - v2.0.7	You must first upgrade to 2.0.8 or 2.0.10 by following the *instructions* for your specific Faspex version. Please contact *Technical Support* on page 175 if you do not have the requisite installer.
Older than v1.6	If your current installation of Faspex Server is older than version 1.6, please contact *Technical Support* on page 175 for assistance. *Be sure to obtain your MySQL and svcAspera passwords before upgrading Faspex Server. You will need them during the installation process.*

First-time Installation

Install Faspex Server on your system for the first time.

Before beginning the installation process, you must be logged into your computer as an administrator *(or domain administrator if you are in an Active Directory environment)*. During the installation process, you will set up the following key components:

- Aspera Enterprise Server 3.0+
- Aspera Faspex Server 3.5+

WARNING: Due to incompatible common components, Aspera Console and Aspera Faspex Server 2.X+ **CANNOT** be installed on the same machine. Aspera does not support this combination. If you are running an older version of Faspex Server (pre-2.X) and Console on the same machine, please contact *Aspera Technical Support* to move one of the applications to another system.

1. Determine whether or not your Aspera Faspex Server will have a domain name

   Before continuing with the installation process, determine whether or not you will be configuring Faspex Server with a domain name. If your Faspex Server is configured to identify itself by IP address (rather than by domain name), then the URLs in your notification emails will contain an IP address (e.g. "https://10.0.0.1/aspera/faspex"). Some Web-based email services (e.g. Yahoo or Ymail, Hotmail, etc.) have been known to automatically flag emails containing IP address links as "Spam," and will move them to your Junk/Spam folder. For this reason, Aspera recommends creating a domain name for your Faspex Server. If you do not have a domain name immediately available, then you can initially configure Faspex with an IP address and then change it to use a domain name later. If you know that you will not be setting up a domain name, then make sure that users add your Faspex "From" email address (e.g. faspex_admin@yourcompany.com) to their address book and/or contact list. Doing so typically "white-lists" the address so that emails from your Faspex Server are not automatically flagged and routed to your users' Junk/Spam boxes.

CAUTION: Do not configure your Faspex server to use a domain name or hostname that contains underscore characters. Doing so could prevent you from logging into the server or cause other connectivity problems. Internet standards for domain names and hostnames do not support underscore characters.

2. Upgrade Windows Installer to version 4 or higher

   The Faspex installer requires *Windows Installer version 4 or higher*. You can download the latest version of Windows Installer and corresponding instructions from *http://www.microsoft.com/downloads/details.aspx?FamilyId=5A58B56F-60B6-4412-95B9-54D056D6F9F4*.

3. Download the requisite Aspera installers

   Download the *Enterprise Server* and *Faspex Server* installers from the following locations (note that you will be required to input your organization's Aspera login credentials to gain access):

   - **Enterprise Server:** *http://asperasoft.com/en/downloads/1*
   - **Faspex:** *http://asperasoft.com/en/downloads/6*

   If you need help determining your organization's access credentials, please contact *Technical Support*.

4. Install Aspera Enterprise Server and license.

   Follow the steps in the Enterprise Server 3.0+ or Connect Server v3.0+ Administrator's Guide to install your software and set up your license. Note that if you are installing Enterprise Server on a remote computer, then you do not need to install it locally. If you are not using a remote transfer server, then complete the installation of Enterprise Server on your local machine and go to the next step. Otherwise, install Enterprise Server on the remote computer and review the topic "*Setting up your Remote Server*" before going to the next step.

5. Secure your SSH server

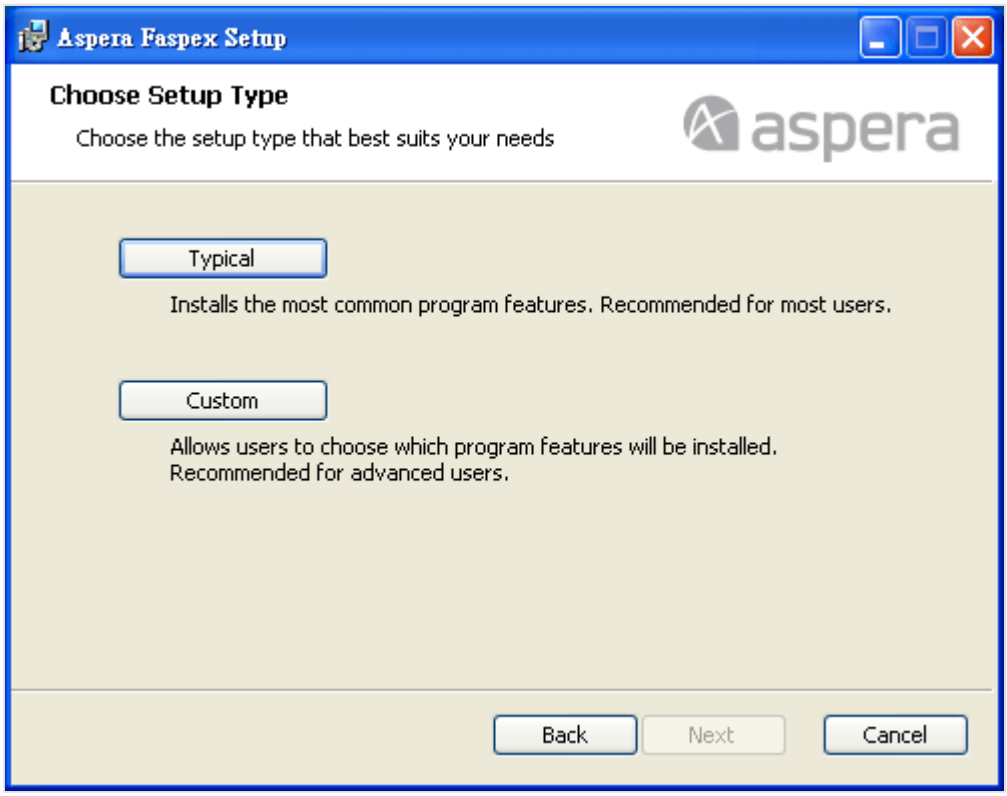
   Keeping your data secure is critically important. As such, Aspera **strongly encourages** you to take additional steps in setting up and configuring your SSH server so that it is protected against common attacks. For detailed instructions on securing your SSH server, please refer to *Securing your SSH Server* on page 19 before continuing with your Faspex Server installation.

6. Install Faspex Server

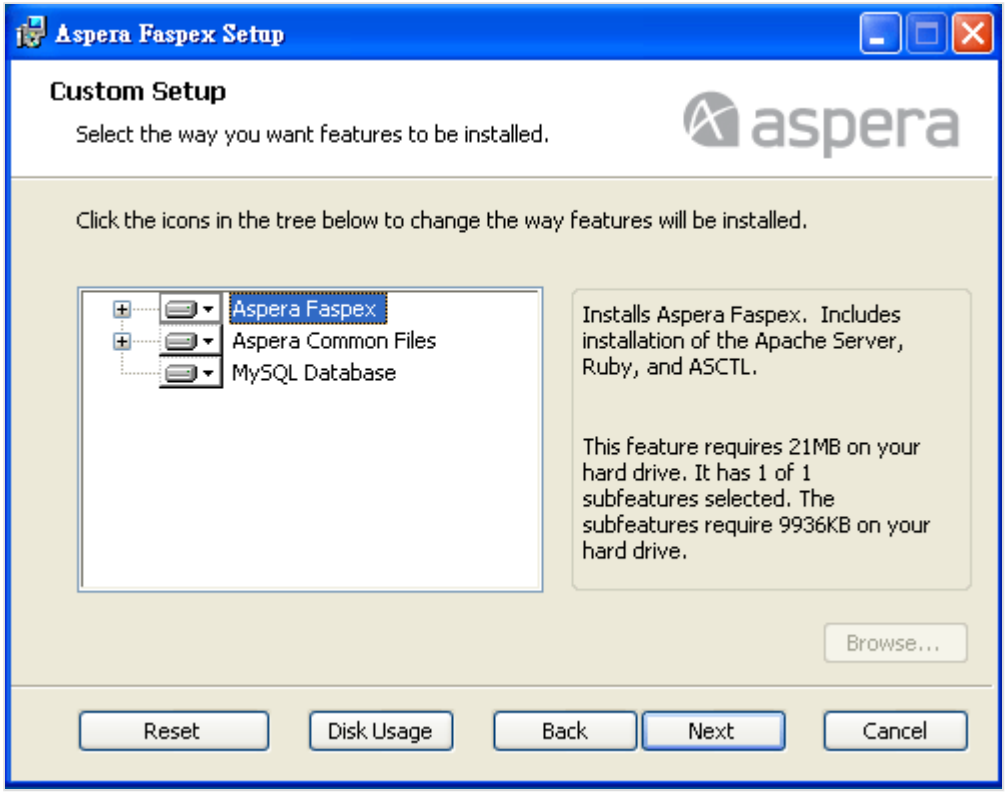
   After downloading the Faspex Server installer, double-click it to begin the installation process. If your Windows Operating System has User Account Control (UAC) enabled, confirm or enter the administrator's password to allow the installer to make changes to your computer. After the license agreement screen, select your desired *setup type*. You may select **Typical** or **Custom**. Setup types are described below.

Option	Description
Typical	Install all required components, including the Faspex application, common files (Ruby and MySQL) and Faspex's MySQL database.

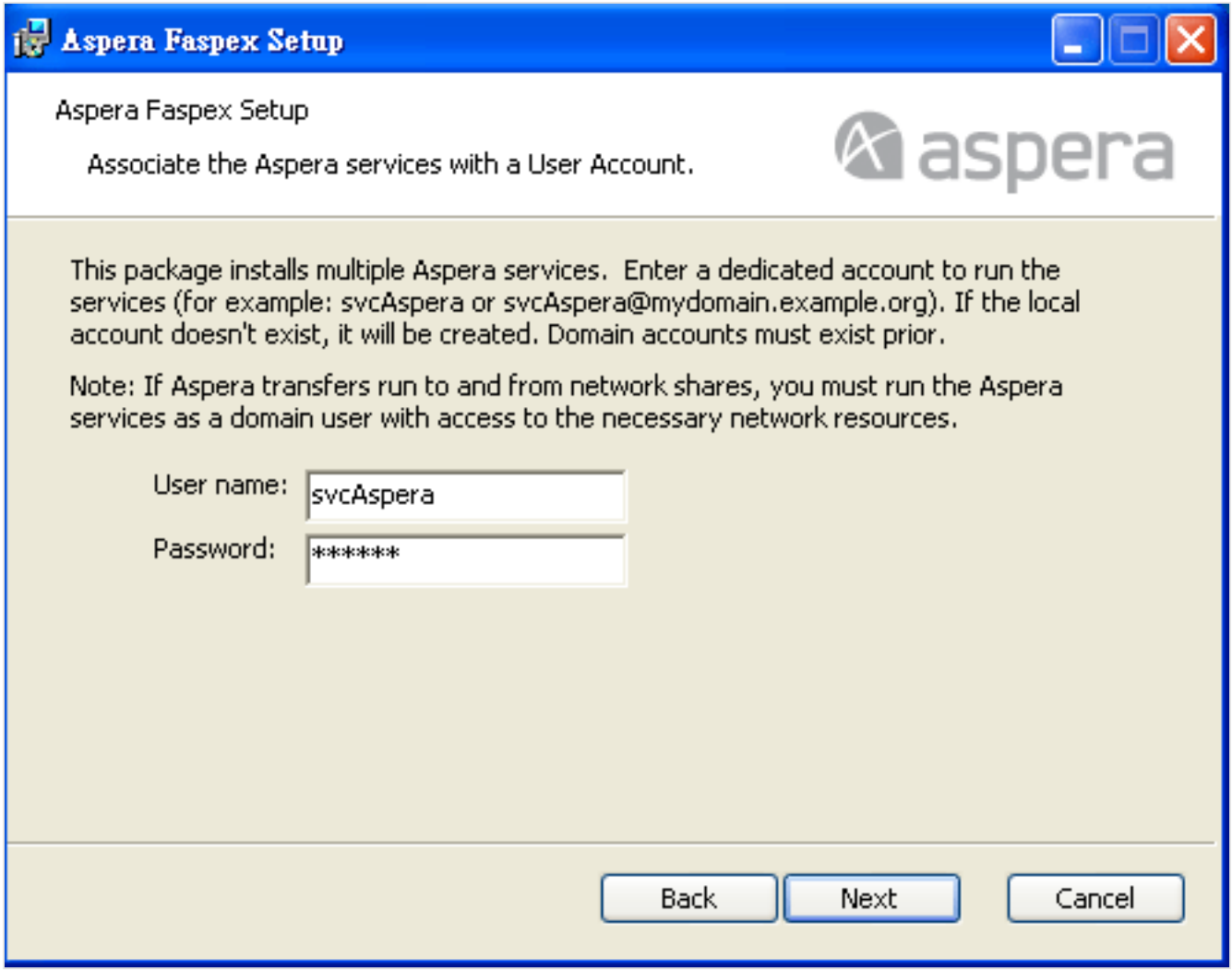
Option	Description
Custom	Select individual components to install; in which event, you may use your existing installation(s) of Ruby, MySQL or Faspex's MySQL database.



If you selected the **Custom** setup type, identify which Faspex Server optional features you want to install.

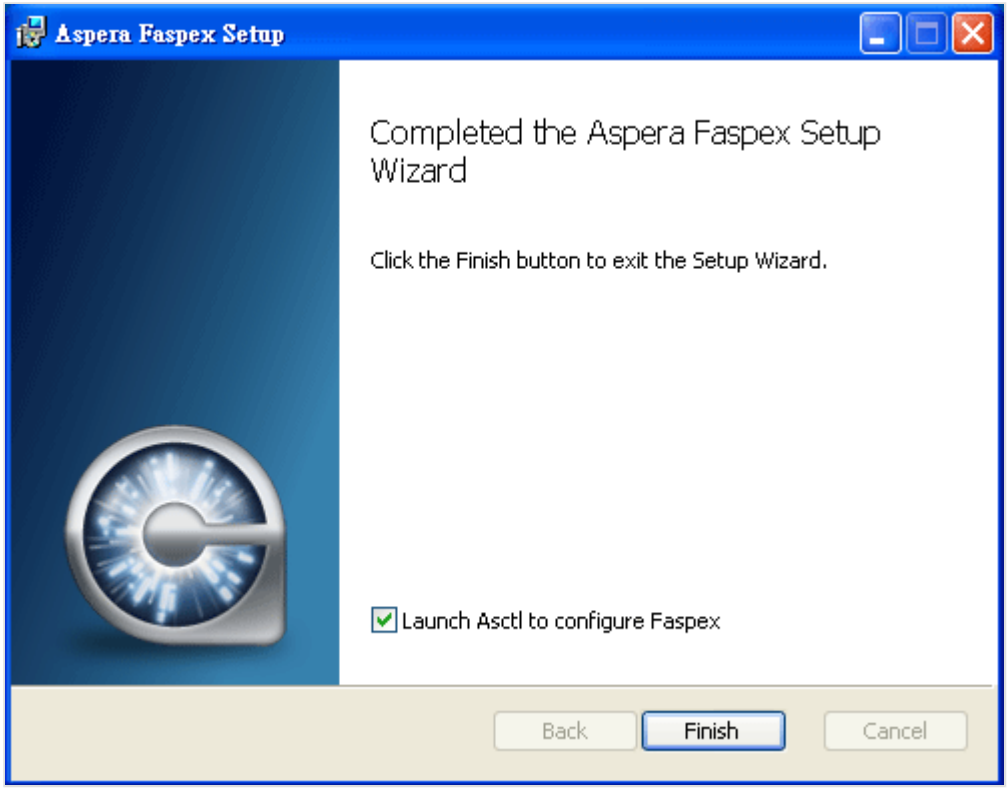


On Windows XP 64-bit, Vista, 2003, 2008 and 7, the installer will then prompt you to create or update an Aspera service account that runs the services for Aspera products (*Aspera Central, Aspera HTTPD, OpenSSH Service (if installed), Aspera Sync*). By default, the user name is *svcAspera*. If the server is configured to accept the domain user login, use a domain account that has been added to the local administrator's group to run the services. On Windows XP 32-bit, instead of creating a user account, you may check the option *Run Aspera services as a local SYSTEM account* to run these services by the local user "SYSTEM". Otherwise, enter the Aspera service account username and password that you created for your installation of Aspera Enterprise Server or Connect Server and click the **Next** button. If the existing user's password you have entered is incorrect, or you wish to change the Aspera service user, refer to *Updating Aspera Service Account* on page 157.



7. Launch *asctl* to continue Faspex setup process

   Once the "Aspera Faspex Setup Wizard" completes, you will receive a prompt with a checkbox and a *Finish* button.



By default, the *Launch asctl to continue the Faspex setup* checkbox is turned on. Once you click *Finish*, the Faspex installer will automatically run the setup command. Follow the configuration instructions to complete the setup. If you do not want to run the setup command automatically, then uncheck (turn off) the *Launch asctl to continue the Faspex setup* checkbox.

IMPORTANT NOTE: If you would like to configure a *remote* transfer server (i.e. your Faspex Web server and Aspera Enterprise Server are on different machines), select *detailed* setup.

If Faspex doesn't automatically run the setup command or an error halts the process, then you can run the command manually, as shown below.

```
> asctl faspex:setup
```

8. (*Perform only if you are configuring Faspex to communicate with a remote transfer server*) Set up your remote transfer server.

   Follow the steps in the topic "*Setting up your Remote Server*" to prepare your remote machine.

Your Faspex Server installation is now complete. To access the Faspex web interface, go to the following address within a browser window:

```
http://<server-ip-or-name>/aspera/faspex
```

Upgrade Procedure

Upgrade your existing Faspex Server

IMPORTANT NOTE: If you are running Aspera Enterprise Server for Isilon OneFS, do not upgrade to Faspex v3.0+! You should not upgrade until Aspera Enterprise Server 3.x is released for the Isilon OneFS Maverick platform (64-bit).

This topic demonstrates the process for upgrading to Faspex v3.0+. If you have not done so already, please review the *Faspex Upgrade Checklist*. You must meet the prerequisites listed in *Faspex Upgrade Checklist* before attempting to upgrade to Faspex v3.0+. If you are upgrading between Faspex v2.5.3 and v3.0+, then you must install an updated license. To obtain the new, FREE license, please contact *Aspera Technical Support*. Once you have obtained your new license, you must copy it into the Faspex Server license directory and restart Faspex, as described in the topic *License* on page 64.

WARNING: Due to incompatible common components, Aspera Console and Aspera Faspex Server 2.X+ **CANNOT** be installed on the same machine. Aspera does not support this combination. If you are running an older version of Faspex Server (pre-2.X) and Console on the same machine, please contact *Aspera Technical Support* to move one of the applications to another system.

1. Back up your existing Faspex database

   To back up your existing Faspex Server database, open a command prompt (**Start Menu** > **All Programs** > **Accessories** > **Command Prompt**) and run the following command:

   ```
   > asctl faspex:backup_database
   ```

   Please see *Save/Restore* for additional instructions and information on backing up your existing Faspex Server database.

2. Upgrade Windows Installer to version 4 or higher

   The Faspex Server installer requires *Windows Installer* version 4+ for successful configuration. You may download the latest version of Windows Installer (as well as view instructions) from the following location:

   http://www.microsoft.com/downloads/details.aspx?FamilyId=5A58B56F-60B6-4412-95B9-54D056D6F9F4

3. Download and run the latest Enterprise Server installer

   Download the latest Enterprise Server installer from the link below (note that you will be required to input your organization's Aspera login credentials to gain access):

   http://asperasoft.com/en/downloads/1

If you need help determining your organization's access credentials for downloading software from the Aspera website, then please contact *Technical Support*.

IMPORTANT NOTE: Faspex requires Enterprise Server or Connect Server version 3.0+. If your system has an earlier version of Enterprise Server or Connect Server installed, then you will need to download the latest version and upgrade your software.

Once downloaded, run the installer and follow the on-screen instructions to upgrade Enterprise Server or Connect Server to the latest version.

4. Stop all services

   Before upgrading, stop all Faspex-related services, including Faspex, MySQL, and Apache. Use the following command:

   ```
   > asctl all:stop
   ```

   IMPORTANT NOTE: If you are running Aspera Console on the same machine, these commands will also shut down Console.

5. Download and run the current Faspex installer

   Download the current Faspex installer from *http://asperasoft.com/en/downloads/6* (note that you will be required to input your organization's Aspera login credentials to gain access). After downloading, run the installer, and follow the instructions to perform the upgrade.

6. Launch *asctl* to continue Faspex setup process

   Once the "Aspera Faspex Setup Wizard" completes, you will receive a prompt with a checkbox and a *Finish* button. By default, the *Launch asctl to continue the Faspex setup* checkbox is turned on. Once you click *Finish*, the Faspex installer will automatically run the upgrade command. Follow the configuration instructions to complete the upgrade. If you do not want to run the upgrade command automatically, then uncheck (turn off) the *Launch asctl to continue the Faspex setup* checkbox.

   IMPORTANT NOTE: If Faspex doesn't automatically run the upgrade command or an error halts the process, then you can run the command manually, as shown below.

   ```
   > asctl faspex:upgrade
   ```

   Please note that the configuration program will ask you whether you want to perform a *streamlined* or *detailed* setup process. Select *detailed* for advanced configuration options.

IMPORTANT NOTE: During an upgrade on Windows 2008 32-bit, Apache may report an error when attempting to restart (*"Apache HTTPD Server (Aspera): The application has failed to start because its side-by-side configuration is incorrect. Please see the application event log for more detail."*). To remedy, install the *Microsoft Visual C++ 2008 SP1 Redistributable Package (x86) package*.

7. Back up your new Faspex Server database

   Aspera recommends backing up your new Faspex Server database. Please use the following command to do so:

   ```
   > asctl faspex:backup_database
   ```

   For more information about database backup, see *Save/Restore*.

8. Reset your custom SSH port setting (if necessary)

   Upgrading faspex does not preserve SSH port settings in faspex. By default, the faspex port setting for SSH is 33001. If you set a custom value in your previous version, such as 22, you need to reset this in your **aspera.conf** file. To do so, add the following line to the **<server>** section of **aspera.conf**:

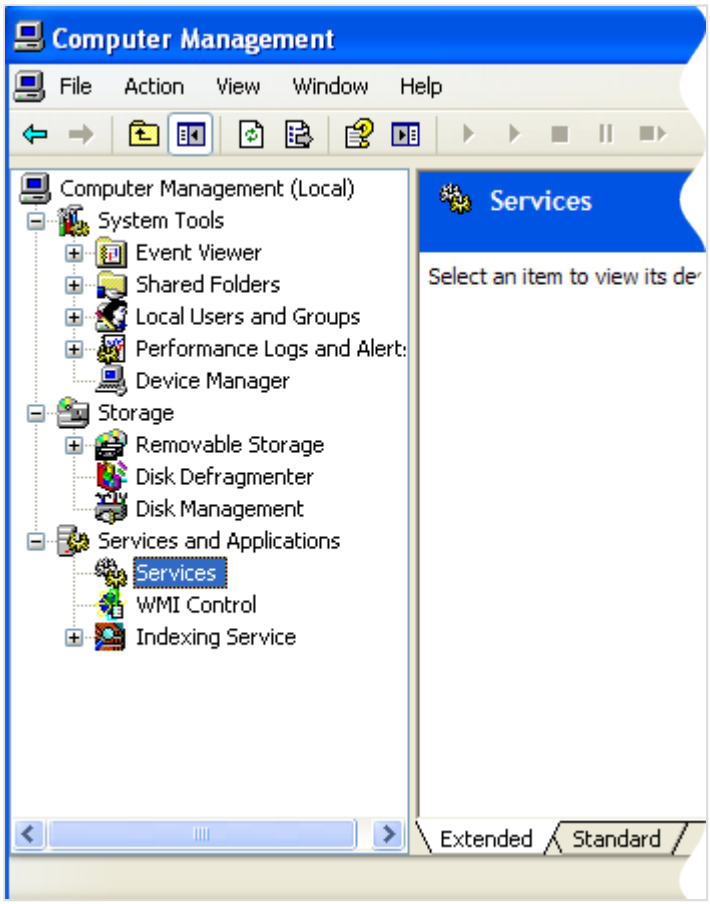
   ```
   <ssh_port>port_number</ssh_port>
   ```

   The **aspera.conf** file can be found in the following location:

OS Version	File Location
32-bit Windows	`C:\Program Files\Aspera\Enterprise Server\etc\aspera.conf`
64-bit Windows	`C:\Program Files (x86)\Aspera\Enterprise Server\etc\aspera.conf`

   After modifying **aspera.conf**, restart **Aspera Central** and **Aspera NodeD** services.

   You can restart these services from the Windows Computer Management window, accessible from **Manage** > **Services and Applications** > **Services** .



Your Faspex Server upgrade is now complete. To update your license, see *License* on page 64.

Securing your Faspex Server

Securing your Faspex Server

Configuring the Firewall

Firewall settings required by the product.

Your Aspera transfer product requires access through the ports listed in the table below. If you cannot establish the connection, review your local corporate firewall settings and remove the port restrictions accordingly.

Product	Firewall Configuration
Faspex Server	An Aspera server runs one SSH server on a configurable TCP port *(22, by default, for Aspera Server 2.6, and 33001, by default, for Aspera Server 2.7+)*. **IMPORTANT NOTE:** Aspera strongly recommends running the SSH server on a non-default port to ensure that your server remains secure from SSH port scan attacks. Please refer to the topic *Securing your Faspex Server* on page 18 for detailed instructions. Your firewall should be configured as follows: • To ensure that your server is secure, Aspera strongly recommends allowing inbound connections for SSH on TCP/33001 (or on another non-default, configurable TCP port), and disallowing inbound connections on TCP/22. If you have a legacy customer base utilizing TCP/22, then you can allow inbound connections on both ports. Please refer to the topic *Securing your Faspex Server* on page 18 for details. • Allow inbound connections for *fasp* transfers, which use UDP/33001 by default, although the server may also choose to run *fasp* transfers on another port. • If you have a local firewall on your server (like `Windows Firewall`), verify that it is not blocking your SSH and *fasp* transfer ports (e.g. TCP/UDP 33001). • For Faspex's Web UI, allow inbound connections for HTTP and/or HTTPS Web access (e.g. TCP/80, TCP/443). The firewall on the server side must allow the open TCP port to reach the Aspera server. **Note that no servers are listening on UDP ports.** When a transfer is initiated by an Aspera client, the client opens an SSH session to the SSH server on the designated TCP port and negotiates the UDP port over which the data transfer will occur. For Aspera servers that have multiple concurrent clients, the *Windows* operating system does not allow Aspera's *fasp* protocol to reuse the same UDP port for multiple connections. Thus, if you have multiple concurrent clients and your Aspera server runs on *Windows*, then you must allow inbound connections on a range of UDP ports, where the range of ports is equal to the

Product	Firewall Configuration
	maximum number of concurrent *fasp* transfers expected. These UDP ports should be opened incrementally from the base port, which is UDP/33001, by default. **For example, to allow 10 concurrent *fasp* transfers, allow inbound traffic from UDP/33001 to UDP/33010.**
Client	Typically, consumer and business firewalls allow direct outbound connections from client computers on TCP and UDP. There is no configuration required for Aspera transfers in this case. In the special case of firewalls disallowing direct outbound connections, typically using proxy servers for Web browsing, the following configuration applies: • Allow outbound connections from the Aspera client on the TCP port (*TCP/33001*, by default, when connecting to a *Windows* server, or on another non-default port for other server operating systems). • Allow outbound connections from the Aspera client on the *fasp* UDP port (33001, by default). • If you have a local firewall on your server (like `Windows Firewall`), verify that it is not blocking your SSH and *fasp* transfer ports (e.g. TCP/UDP 33001). **IMPORTANT NOTE:** Multiple concurrent clients cannot connect to a Windows Aspera server on the same UDP port. Similarly, multiple concurrent clients that are utilizing two or more user accounts cannot connect to a Mac OS X or FreeBSD Aspera server on the same UDP port. If connecting to these servers, you will need to allow a range of outbound connections from the Aspera client (that have been opened incrementally on the server side, starting at UDP/33001). For example, you may need to allow outbound connections on UDP/33001 through UDP/33010 if 10 concurrent connections are allowed by the server.

Securing your SSH Server

Secure your SSH server to prevent potential security risks.

Introduction

Keeping your data secure is critically important. Aspera **strongly encourages** you to take additional steps in setting up and configuring your SSH server so that it is protected against common attacks. Most automated robots will try to log into your SSH server on Port 22 as *Administrator*, with various brute force and dictionary combinations in order to gain access to your data. Furthermore, automated robots can put enormous loads on your server as they perform thousands of retries to break into your system. This topic addresses steps to take in securing your SSH server against potential threats, including changing the default port for SSH connections from TCP/22 to TCP/33001.

Why Change to TCP/33001?

It is well known that SSH servers listen for incoming connections on TCP Port 22. As such, Port 22 is subject to countless, unauthorized login attempts by hackers who are attempting to access unsecured servers. A highly effective

deterrent is to simply turn off Port 22 and run the service on a seemingly random port above 1024 (and up to 65535). To standardize the port for use in Aspera transfers, we recommend using **TCP/33001**.

Please note that for Aspera Enterprise or Connect Server version 2.6 or older, your transfer product ships with OpenSSH listening on TCP/22. For Aspera Enterprise or Connect Server 2.7+, your transfer product ships with OpenSSH listening on *both* TCP/22 and TCP/33001. For both versions, Aspera recommends disabling TCP/22 and only exposing TCP/33001 or another non-default port.

IMPORTANT NOTE: You need *Administrator* access privileges to perform the steps below.

1. Locate and open your system's *SSH configuration* file

   Open your *SSH configuration* file with a text editor. You will find this file in the following system location:

OS Version	Path
32-bit Windows	`C:\Program Files\Aspera\Enterprise Server\etc\sshd_config`
64-bit Windows	`C:\Program Files (x86)\Aspera\Enterprise Server\etc\sshd_config`

2. Add new SSH port

IMPORTANT NOTE: Before changing the default port for SSH connections, please verify with your network administrators that TCP/33001 is open.

   The OpenSSH suite included in the installer uses TCP/22 and TCP/33001 as the default ports for SSH connections. Aspera recommends disabling TCP/22 to prevent security breaches of your SSH server.

   Once your client users have been notified of the port change (from TCP/22 to TCP/33001), you can disable Port 22 in your `sshd_config` file. To disable TCP/22 and use only TCP/33001, comment-out Port 22 in your `sshd_config` file.

```
...
#Port 22
Port 33001
...
```

3. Disable non-admin SSH tunneling

IMPORTANT NOTE: The instructions below assume that OpenSSH 4.4 or newer is installed on your system. For OpenSSH 4.4 and newer versions, the "Match" directive allows some configuration options to be selectively overridden if specific criteria (based on user, group, hostname and/or address) are met. If you are running an

OpenSSH version older than 4.4, the "Match" directive will not be available and Aspera recommends updating to the latest version.

In OpenSSH versions 4.4 and newer, disable SSH tunneling to avoid potential attacks; thereby only allowing tunneling from *Administrator group* users. To disable non-admin SSH tunneling, add the following lines at the end of the `sshd_config` file:

```
...
AllowTcpForwarding no
Match Group Administrators
AllowTcpForwarding yes
```

Depending on your `sshd_config` file, you may have additional instances of `AllowTCPForwarding` that are set to the default `Yes`. Please review your `sshd_config` file for other instances and disable as appropriate.

4. Update authentication methods

   Public key authentication can prevent brute force SSH attacks if all password-based authentication methods are disabled. Thus, Aspera recommends disabling password authentication in the `sshd_config` file and enabling private/public key authentication. To do so, add or uncomment `PubkeyAuthentication yes` in the `sshd_config` file and comment out `PasswordAuthentication yes`.

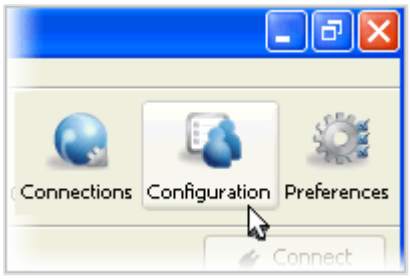
   ```
   ...
   PubkeyAuthentication yes
   #PasswordAuthentication yes
   PasswordAuthentication no
   ...
   ```

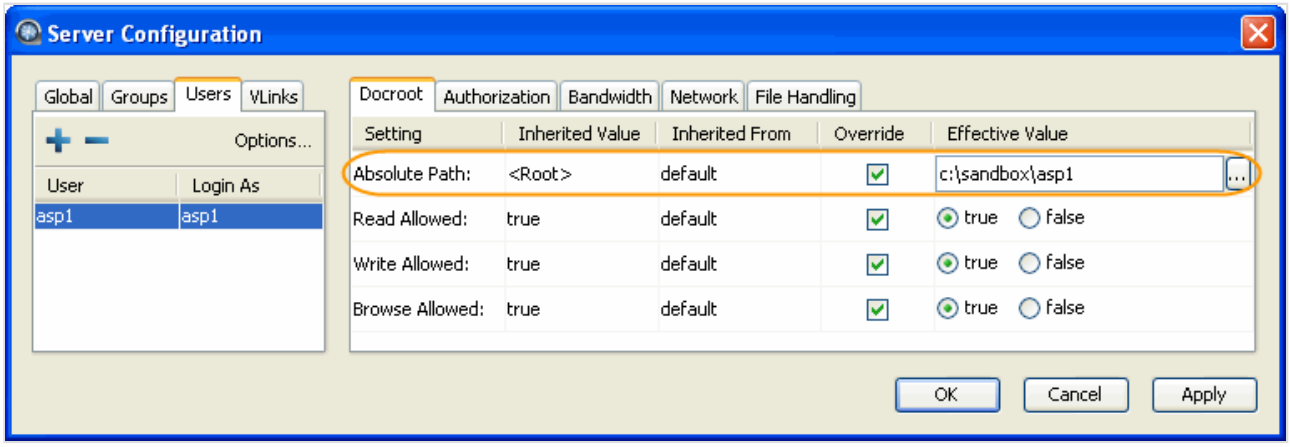
5. Restart the SSH server to apply new settings

   When you have finished updating your SSH server configuration, you must restart the server to apply your new settings. *Restarting your SSH server will not impact currently connected users*. To restart your SSH Server, go to **Control Panel** > **Administrative Tools** > **Services** . Locate the `OpenSSH Service` and click **Restart**.

6. Restrict user access

   Restricting user access is a critical component of securing your server. When a user's docroot is empty (i.e. blank), that user has full access to your server's directories and files. To restrict the user, you must set a non-empty docroot, which automatically changes the user's shell to `aspshell` (Aspera shell). You can do so from the product GUI by going to **Configuration** > **Users** > **Docroot** > **Absolute Path** . Input a path in the blank field and ensure that **Override** is checked.



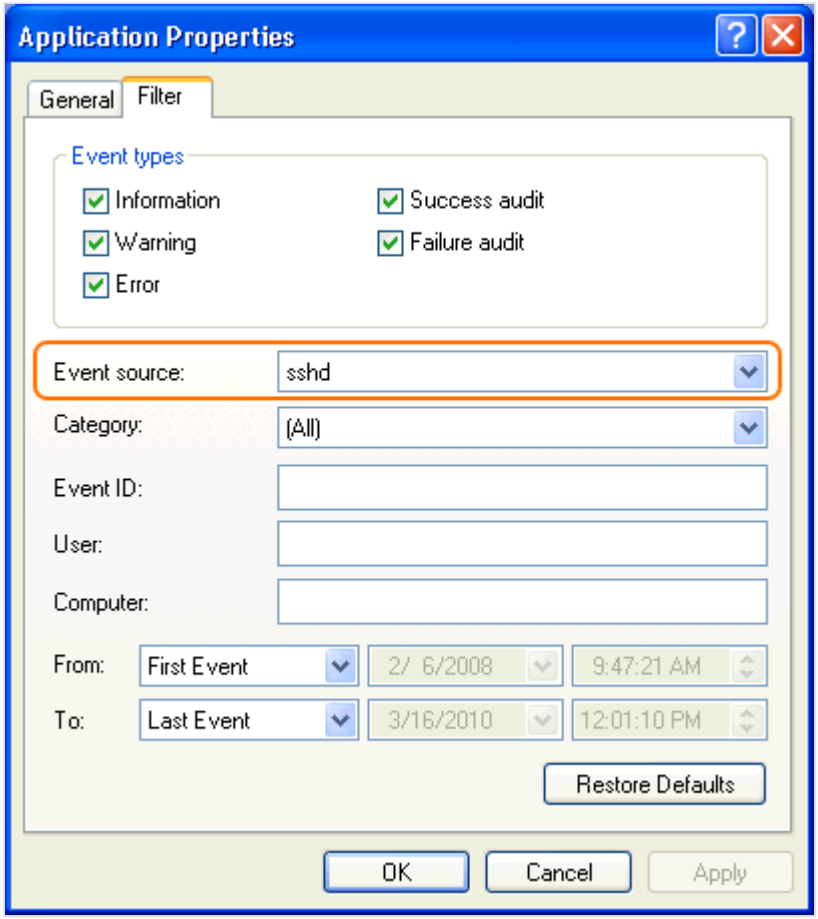


Once you have set the user's docroot, you can further restrict access by disabling read, write and/or browse. You may do so via the product GUI (as shown in the screenshot above).

Field	Description	Values
Absolute Path	The area of the file system (i.e. path) that is accessible to the Aspera user. The default empty value gives a user access to the entire file system.	Path or blank
Read Allowed	Setting this to `true` allows users to transfer from the designated area of the file system as specified by the Absolute Path value.	• `true` • `false`
Write Allowed	Setting this to `true` allows users to transfer to the designated area of the file system as specified by the Absolute Path value.	• `true` • `false`
Browse Allowed	Setting this to `true` allows users to browse the directory.	• `true` • `false`

7. Review your logs periodically for attacks

Aspera recommends reviewing your SSH log periodically for signs of a potential attack. Launch **Control Panel** > **Administrative Tools** > **Event Viewer** . To see only SSH Server events, select **View** > **Filter...** to bring up the filter settings. In **Application Properties** > **Filter** tab, select **sshd** in the **Event source** menu to display only SSH Server events. You may also apply other conditions when needed.



With a filter applied, you can review the logs in the *Event Viewer* main window, or select **Action** > **Save Log File As...** to export a log file using `.txt` or `.csv` format.

Look for invalid users in the log, especially a series of login attempts with common user names from the same address, usually in alphabetical order. For example:

```
...
Mar 10 18:48:02 sku sshd[1496]: Failed password for invalid user alex from 1.2.3.4
 port 1585 ssh2
...
Mar 14 23:25:52 sku sshd[1496]: Failed password for invalid user alice from 1.2.3.4
 port 1585 ssh2
...
```

If you have identified attacks:

- Double-check the SSH security settings in this topic.
- Report attacker to your ISP's abuse email (e.g. `abuse@your-isp`).

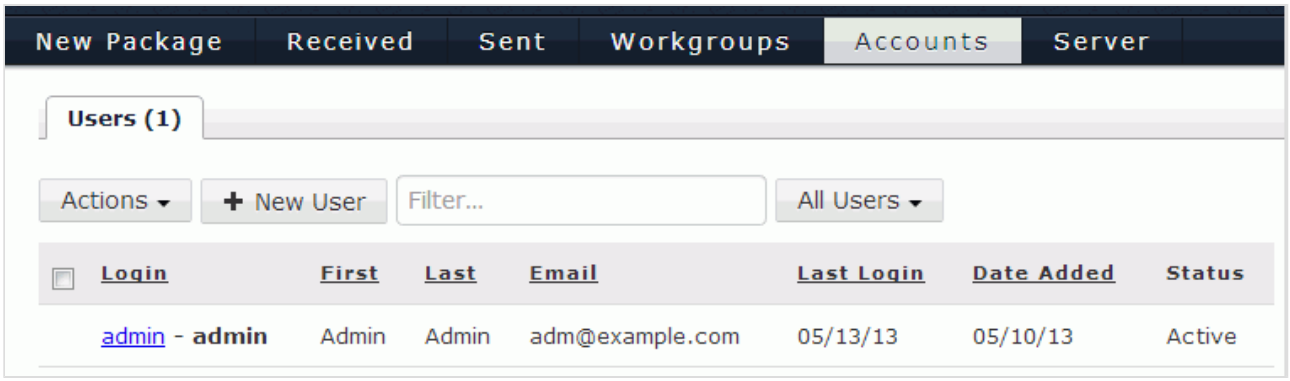
Configure a Secure Faspex

Configure Faspex settings to ensure a secure server.

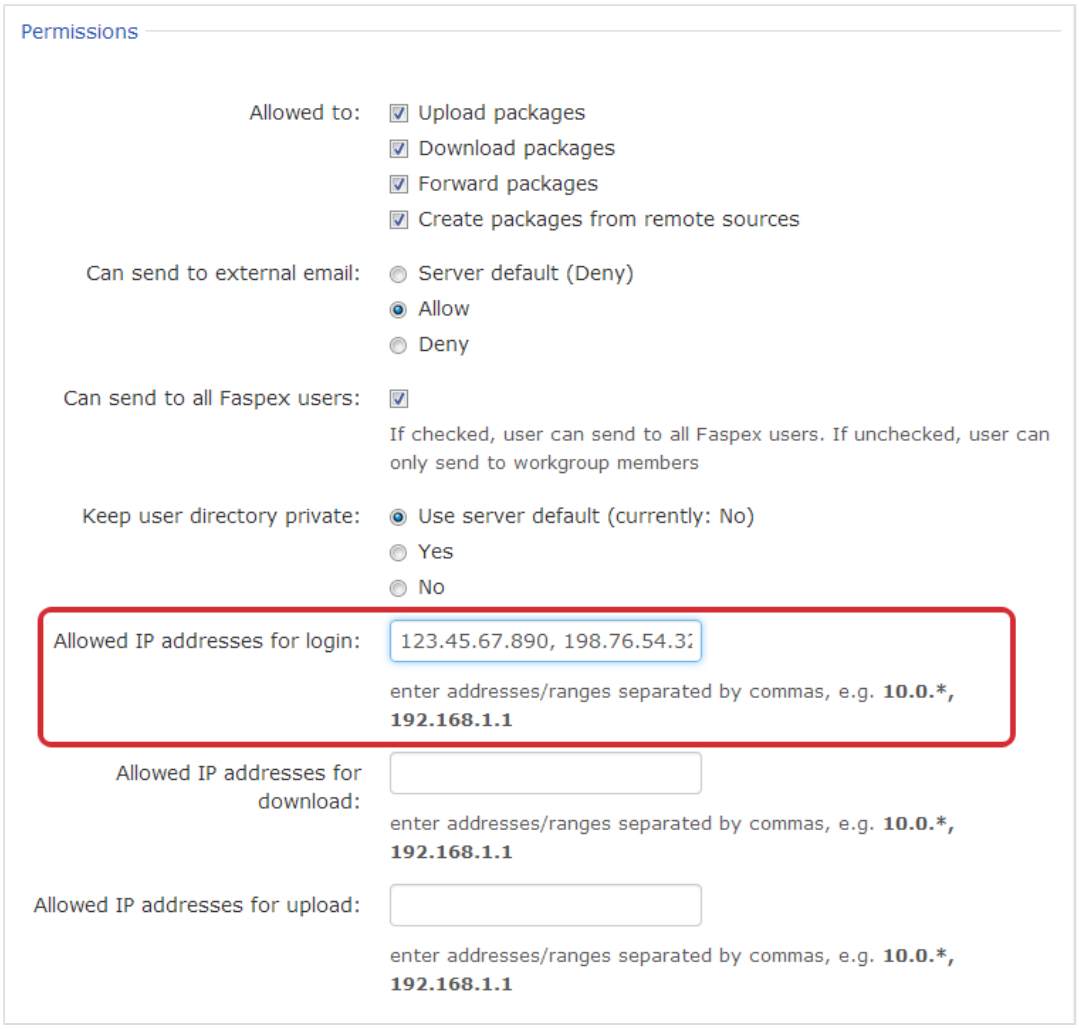
Aspera strongly recommends configuring your Faspex Server settings to ensure that your data remains secure. The following steps are Aspera's recommended security settings for Faspex Server:

1. Complete the steps detailed in the topic *Securing your SSH Server* on page 19.
2. For all Administrator accounts (existing and new), disallow login attempts from unknown IP addresses.

   To update your Admin user permissions, go to **Accounts** and click the corresponding login name(s).



   Within the *Edit User* screen, scroll down to the **Permissions** section and update the **Allowed IP addresses for login** field (input specific office, home, etc. IP addresses). Be sure to click "Save" at the bottom of the page to retain your settings. Perform the same actions when adding new admin users.

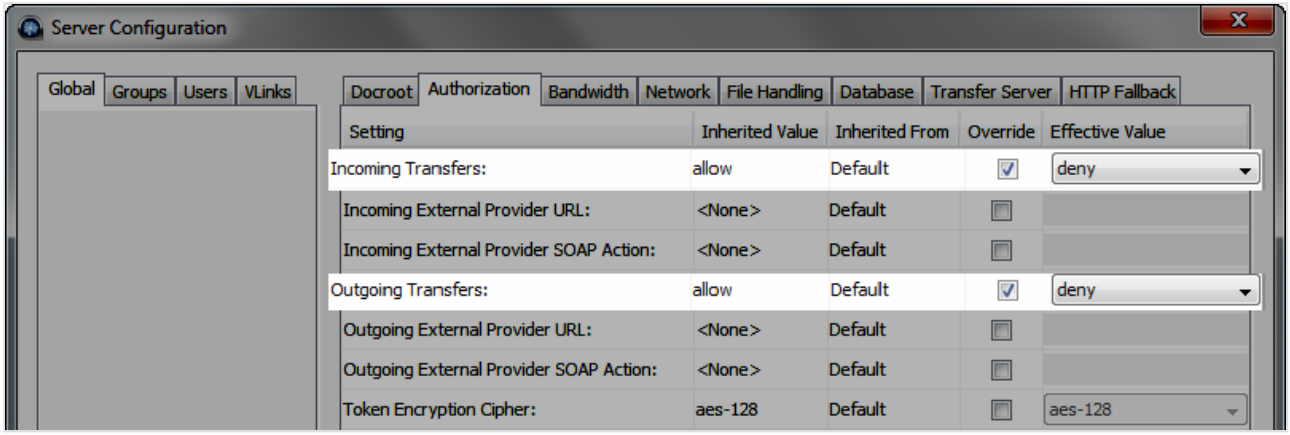


IMPORTANT NOTE: Faspex administrators have the ability to execute post-processing scripts on the server. In the event that an Administrative account is compromised, this capability can be a serious threat to your server's security. As such, Aspera strongly recommends that you update your Administrative user(s)' permissions in order to prevent unauthorized users from executing post-processing on your Faspex server.

3. Update the *Incoming Transfers* and *Outgoing Transfers* **global Authorization** settings for your installation of Aspera Enterprise Server or Connect Server (either through the GUI or by editing aspera.conf)

   Launch Aspera Enterprise Server via **Start menu** > **All Programs** > **Aspera** > **Enterprise Server** > **Enterprise Server**, and then select the "Configuration" button, "Global" tab, and lastly, the *Authorization* tab.

   Override the global, default setting of "allow" for both *Incoming Transfers* and *Outgoing Transfers*, and change both settings to "deny." You can then set transfer permissions on an individual user basis via the *Users* tab.



4. *(Complete this step if your system is a dedicated Faspex Server and is not performing transfers with Enterprise or Connect Server)* Only allow user "*faspex*" within Enterprise Server

   Launch Aspera Enterprise Server via **Start menu** > **All Programs** > **Aspera** > **Enterprise Server** > **Enterprise Server**, and then select the "Configuration" button and "Users" tab. Ensure that *faspex* is the only user listed.

Getting Started

Log into Faspex server and set up your account.

Logging In

Access your Faspex server

1. Navigate to your Faspex Server website in a browser window and input your login credentials.

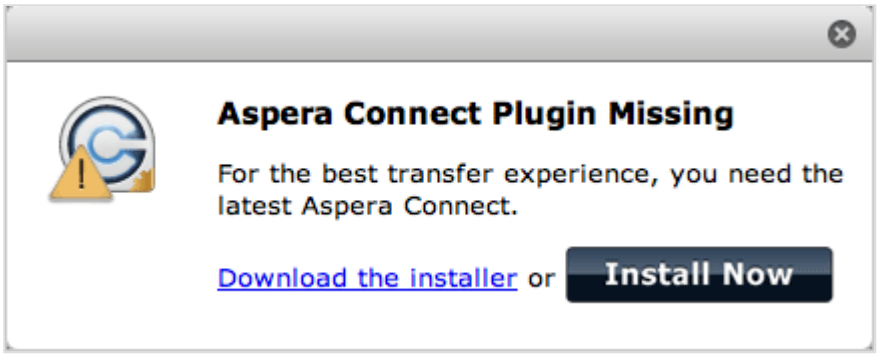
   To access your Faspex Server's web interface within a browser window, go to the domain or IP address that you set up during the installation process. For example:

   - `https://<your-server-ip-or-name>/aspera/faspex`
   - `https://faspex.<your-domain>.com`

   Here, input your Faspex Server username and password, and click the **Login** button to continue.

2. If prompted to do so (after logging in), install the Aspera Connect browser plugin.

   You must have the Aspera Connect browser plugin installed to access the Faspex Server web interface. If Aspera Connect is not detected on your system, you will be prompted to install it.

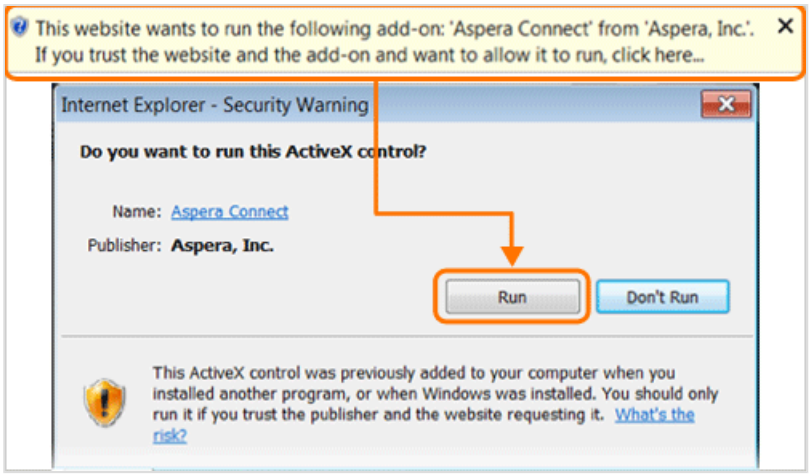


For systems that support Java, clicking the **Install Now** button automatically installs the Aspera Connect browser plugin. When installation has completed, refresh your browser window to check whether or not Aspera Connect has installed successfully. If it has not installed successfully or if your system doesn't support Java, then click the **Download the installer** link to access the Aspera Connect download page (*http://asperasoft.com/connect*). From here, you can download the Aspera Connect installer for your specific operating system.

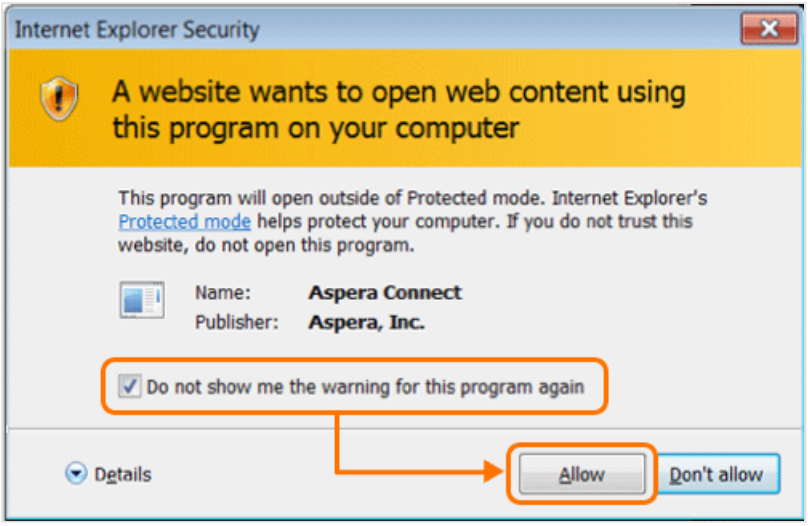
IMPORTANT NOTE: As a Faspex user, you have the option to suppress Aspera Connect's installation from your Faspex **Preferences** page.

3. *(Applicable to Internet Explorer 7+ browser only)* Review Internet Explorer security warnings

If you are accessing the Faspex Server web interface with Internet Explorer (IE) 7+, you will be prompted to run the "Aspera Connect ActiveX control add-on." Click the **Run** button to continue.



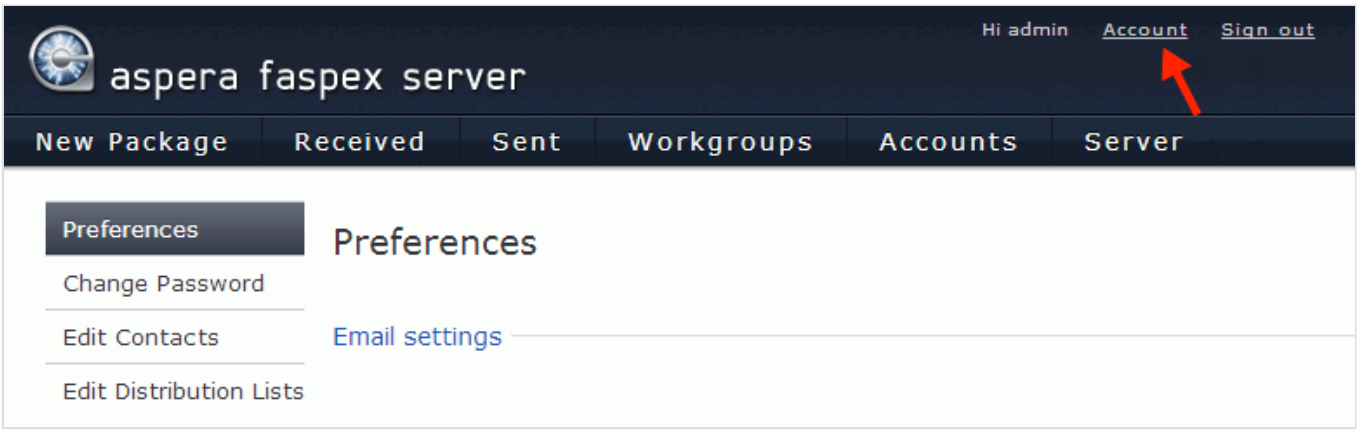
You will also be prompted with an IE security warning when Faspex attempts to launch Aspera Connect. Check the option *Do not show me the warning for this program again*, then click the **Allow** button to continue.



Account (Preferences)

Update Faspex user preferences via the "Account" link.

When logged in, select the **Account** link to update your Faspex account preferences, including email address, notification options, maximum listed rows, and password. **Be sure to click the Save button after editing your preferences.**



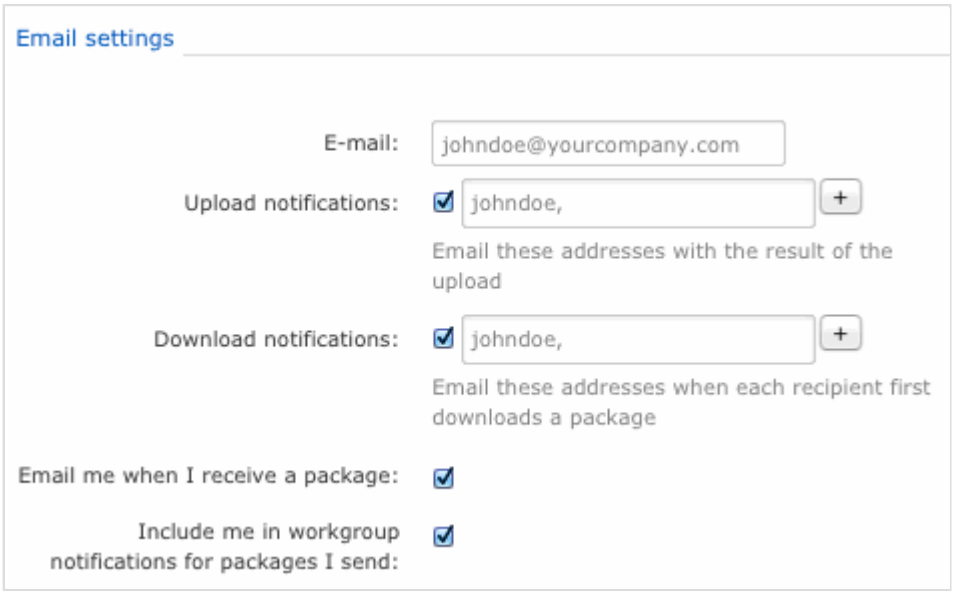
On the left side of the Account screen, you can navigate to the following areas:

- **Preferences**: Change preferences for your email address, notifications, table rows, and Connect prompts.
- **Change Password**: Change your Faspex account password.
- **Edit Contacts**: Delete external email addresses and other contacts that have been added to your contacts list.
- **Edit Distribution Lists**: Create and edit distribution lists for package recipients.

Preferences

Email Settings

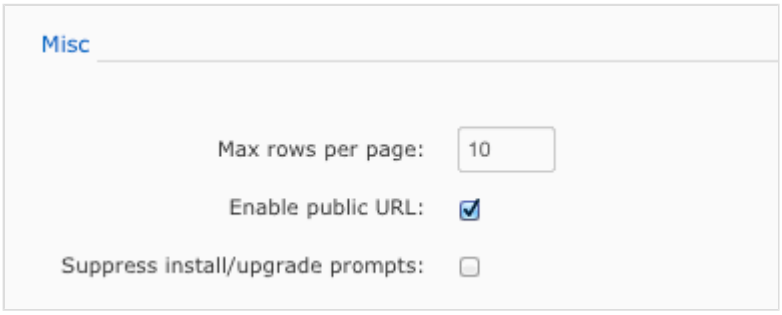
Option	Description
E-mail	Enter your email address to receive electronic notifications from Faspex.
Upload notifications	If you would like to be notified (via email) after you have uploaded a package successfully, enable this checkbox and input your faspex account. You can notify additional users from your contacts list by clicking the **+** button.
Download notifications	If you would like to be notified (via email) after the recipient(s) downloads your package successfully, enable this checkbox and input your faspex account. You can notify additional users from your contacts list by clicking the **+** button.
Email me when I receive a package	Enable if you want Faspex to notify you when new packages are received.
Include me in workgroup notifications for packages I send	Enable if you want Faspex to notify you when a workgroup receives your package(s).



Misc

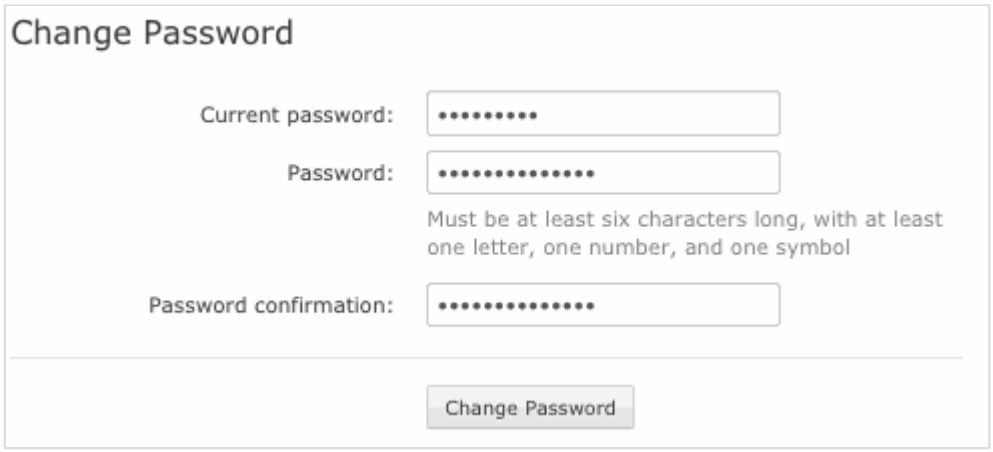
Option	Description
Max rows per page	For a package or an account list, set how many rows will be displayed per page.
Enable public URL	**IMPORTANT NOTE:** This field and checkbox will not appear if **(1)** Public URLs are disabled server-wide or **(2)** Public URLs have been disabled for this particular user.

Option	Description
	A Public URL can be used by external senders to submit packages to registered Faspex users. The benefit of using a Public URL is in the time-savings, such that external senders no longer need to be individually invited to submit a package (although that functionality still exists). When a Public URL is enabled and posted to an email message, instant message, website, etc., the following workflow occurs: **1. The external sender clicks the Faspex user's Public URL.** **2. The sender is directed to page where he or she is asked to enter and submit an email address.** **3. A private link is *automatically* emailed to the sender.** **4. The sender clicks the private link and is automatically redirected to the Faspex-user package submission page.** **5. Once the package is submitted through the private link, the Faspex user receives it.** As a Faspex user, you can enable or disable the **Enable public URL** feature for your account, as long as Public URLs are allowed by your Server Administrator.
Suppress prompts to install or upgrade	If checked, Connect browser plug-in installation/upgrade prompts will be suppressed, regardless of whether Connect is already installed.



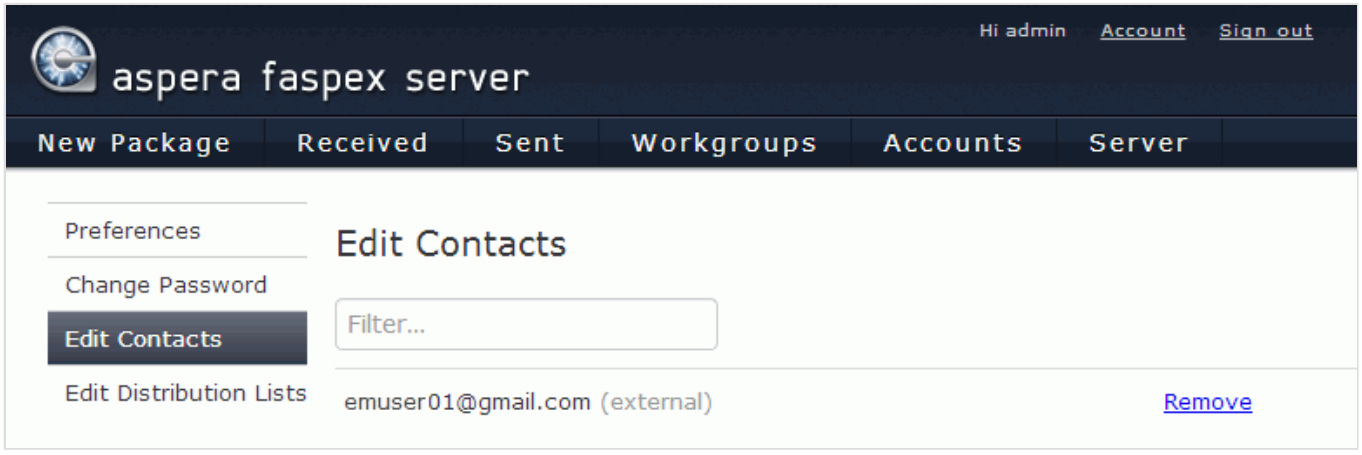
Change Password

Option	Description
Old Password	Enter your current (i.e., old) password.
New Password	Enter a new password. Based on your Faspex Server settings, this password may need to be a *strong* password that contains at least six characters (with a minimum of one letter, one number and one symbol).
Confirm New Password	Repeat your new password and click the **Update Password** button when finished.



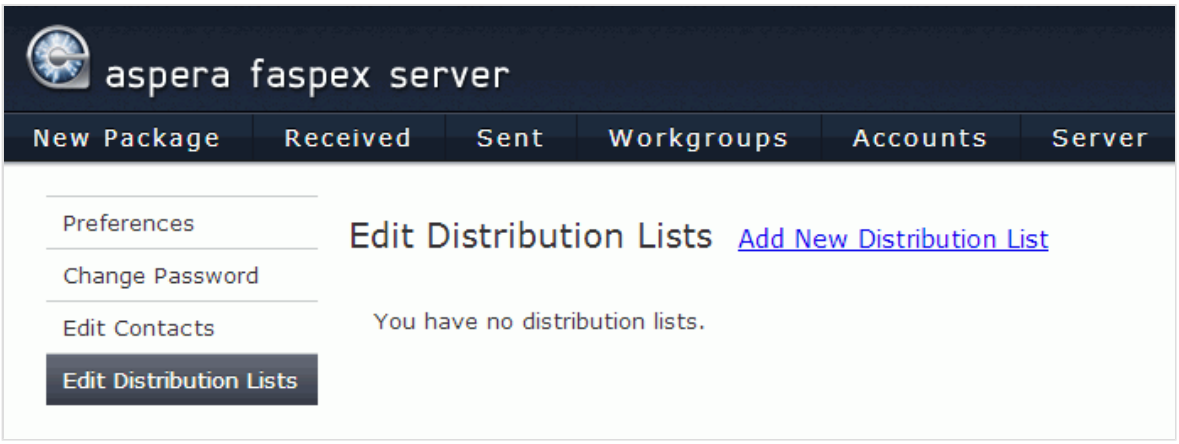
Edit Contacts

If you are permitted to send packages to external email addresses, and you have sent files to a new email address, Faspex automatically saves the recipient in your contact list. If your account has also been configured with **Keep user directory private** set to ON, each recipient of your packages and each sender to you is automatically added to your contact list. To remove external email addresses from your contact list, click the **Remove** link.

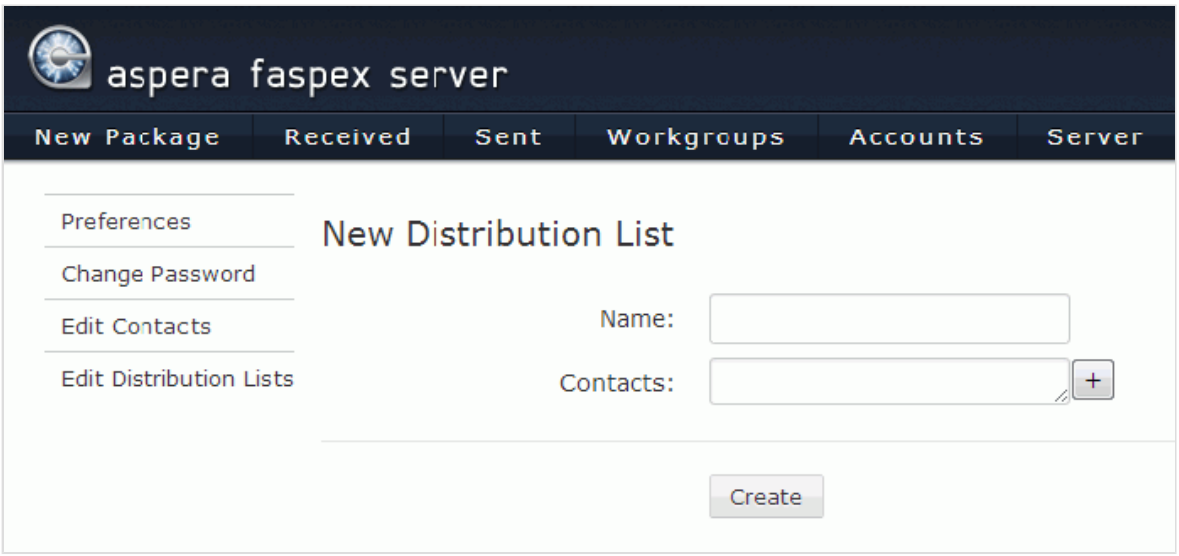


Edit Distribution Lists

When you select Edit Distribution Lists, the display that appears lists your existing distribution lists, if any, and gives you the choice of editing the existing lists or creating a new list.



To create a new list, click the **Add New Distribution List** link. The following display appears:

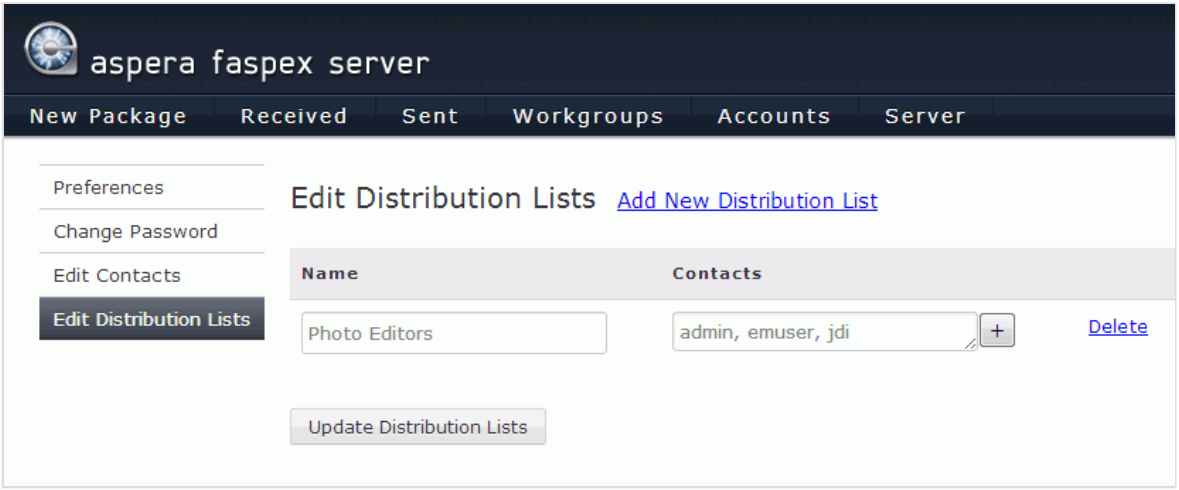


For **Name**, enter a name for your distribution list. For **Contacts**, click + to open a list of user and workgroup names to choose from.

CAUTION:

- Do not choose a name for your distribution list that is the same as a member user or workgroup name.
- A package cannot be sent if any recipient in the distribution list is an invalid user. If a user is external and sending to external users is disabled, the external user would be considered invalid, regardless of whether the email address is active.
- You cannot CC a distribution list. Distribution lists can only be used for regular or private recipients.

To modify or delete a distribution list, go to **Account > Edit Distribution Lists**. In addition to allowing you to add a new distribution list, this will show your existing lists and allow you to change list names, add or remove contacts, or delete the list altogether.


aspera faspex server
New Package
Received
Sent
Workgroups
Accounts
Server
Preferences
Change Password
Edit Contacts
Edit Distribution Lists
Edit Distribution Lists
Add New Distribution List
Name
Contacts
Photo Editors
admin, emuser, jdi
+
Delete
Update Distribution Lists

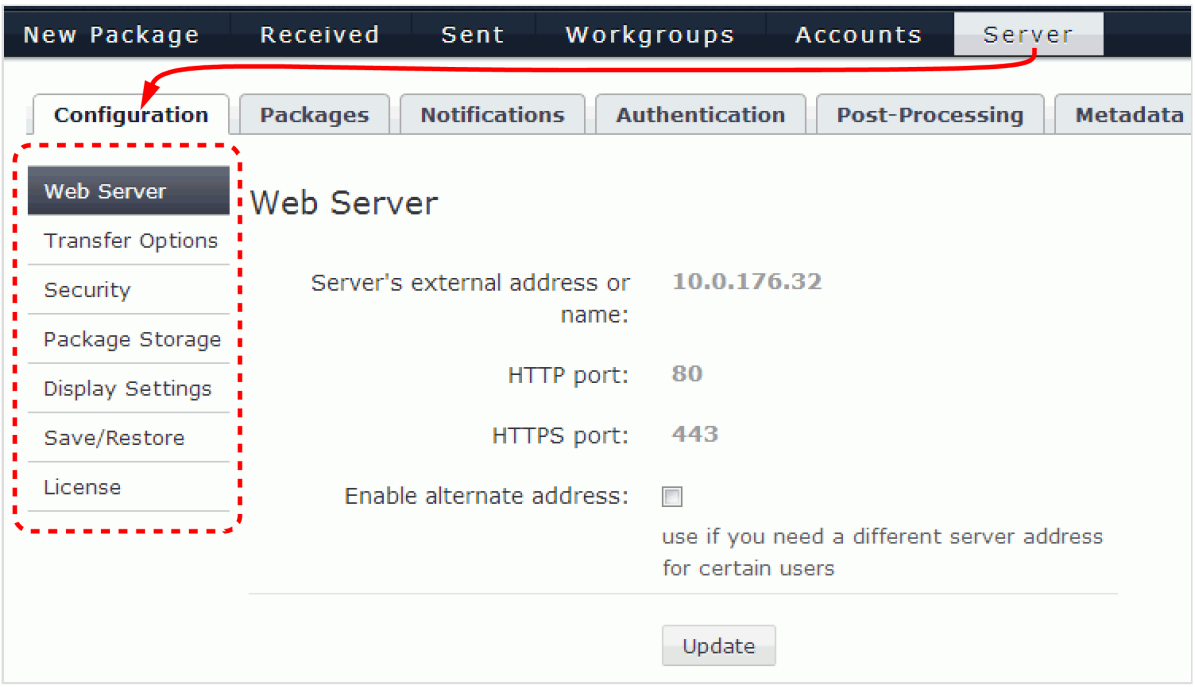
Configuring your Faspex Server

Configure Faspex Server settings including AD, send forms, notifications, and post-processing.

Server Configuration Overview

Configure your Faspex server.

For Administrators, Faspex Server's **Configuration** tab provides access to multiple configuration options. Within the Faspex Server Web UI, go to **Server** > **Configuration** to view and/or modify the following settings:



Topic Link	Configuration Description
Web Server	The Web Server page shows the configuration settings for the Faspex Web UI server, including the IP address or name and HTTP/HTTPS ports that users connect to when accessing the Web UI. Note that this server does not have to be the same system that manages your transfers (the transfer server). If you have a group of external users who must log into Faspex through a different IP address or domain name, you can enable and configure the alternate address or name on this page.
Transfer Options	Update file transfer options, including HTTP fallback, default transfer rates, Aspera Connect browser plugin warnings and server-to-server relay outgoing bandwidth.
Security	Modify security settings for Faspex user accounts, self registration, external senders and encryption.

Topic Link	Configuration Description
Package Storage	Change the default package expiration time, as well as what to do with packages after they are downloaded by recipients.
Display Settings	Update the date format (that which appears in the Faspex Web UI).
Save/Restore	Save and restore your Faspex configuration and database via the Web UI.
License	Upload and/or paste your Aspera Faspex Server license, which is then decoded and displayed on this page.

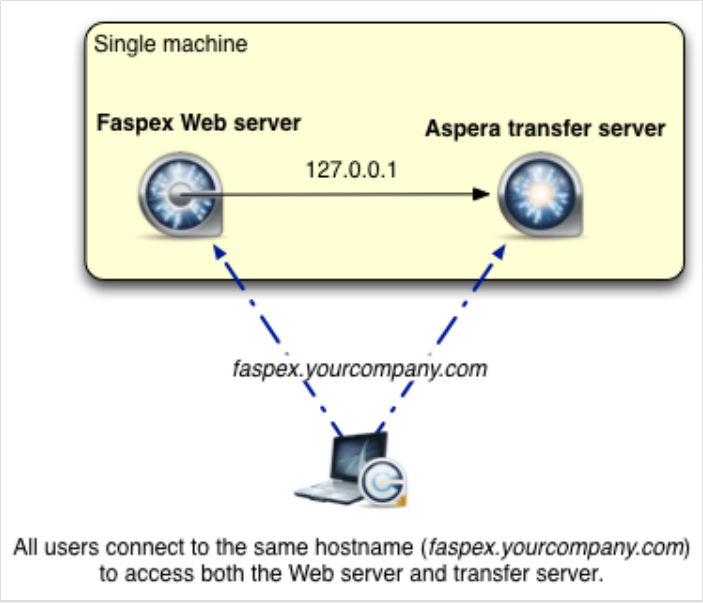
Web Server

Configure the Faspex Web server.

Go to **Server** > **Configuration** > **Web Server** to view and/or modify your settings for the Faspex **Web** server. On this page, the Faspex Web server's IP address or name and HTTP/HTTPS ports are displayed. These settings were initially configured when you first installed Faspex and completed the *asctl* setup process. Note that the Web server does not have to be the same system that manages your transfers (i.e. the *transfer server*). Please refer to the examples below for common Faspex Web server configurations.

Example #1 - Faspex Web server has one address for both internal and external users

In the simplest case, the Faspex Web server is on the same machine as your Aspera transfer server (i.e. Enterprise or Connect Server) and all users--both internal and external--use the same IP address or hostname to connect to Faspex.



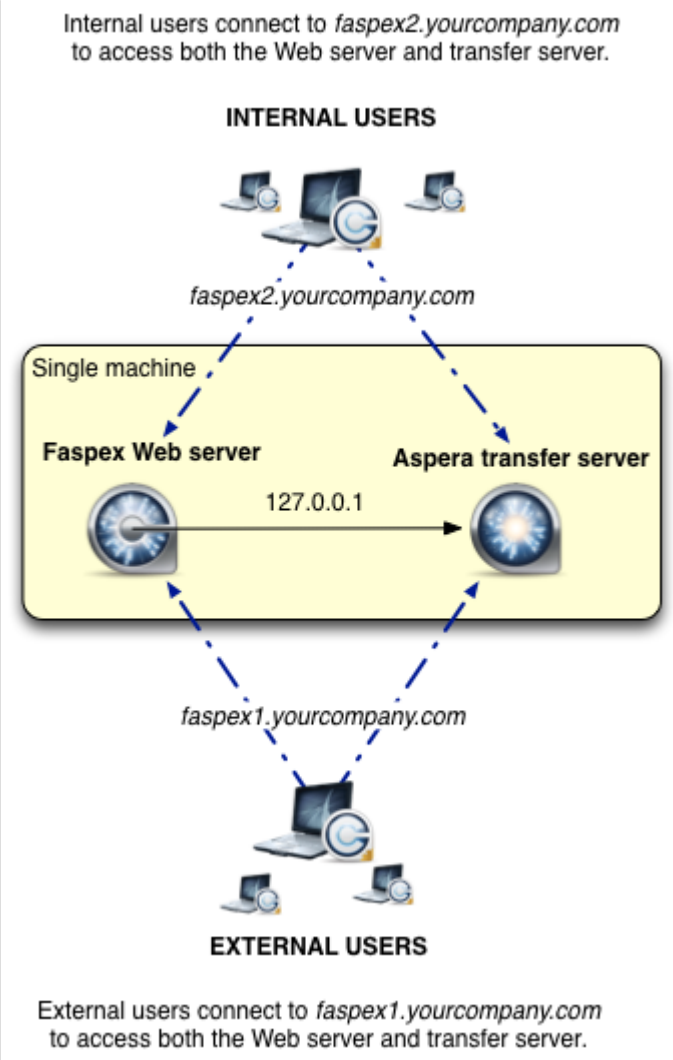
All users connect to the same hostname (*faspex.yourcompany.com*) to access both the Web server and transfer server.

Faspex Web Server Setting	Example #1 Value
External IP address or name	`faspex.yourcompany.com`

Faspex Web Server Setting	Example #1 Value
HTTP Port / HTTPS Port	80 / 443
Enable alternate address	Disabled

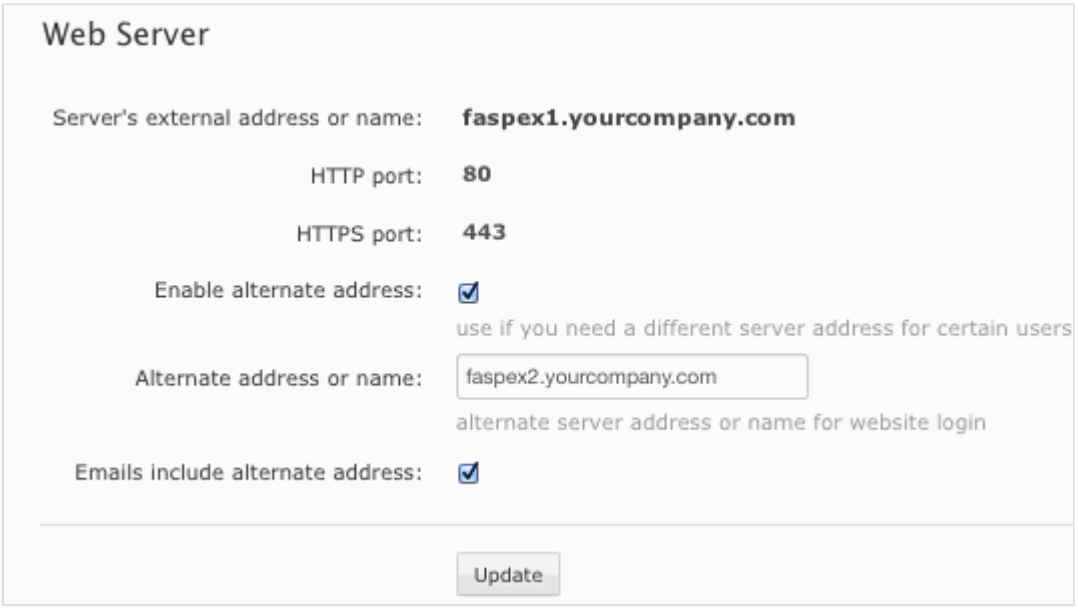
Example #2 - Faspex Web server has an alternate address for internal users

In this case, the Faspex Web server is still on the same machine as your Aspera transfer server (i.e. Enterprise or Connect Server); however, internal and external users connect to Faspex via different URLs due to a company security requirement. Additionally, you would like Faspex package notifications to include a link to the alternate address (which will only resolve for internal users).



Faspex Web Server Setting	Example #2 Value
External IP address or name	`faspex1.yourcompany.com`
HTTP Port / HTTPS Port	80 / 443

Faspex Web Server Setting	Example #2 Value
Enable alternate address	Enabled
Alternate address or name	`faspex2.yourcompany.com`
Emails include alternate address	Enabled



Configuration Option	Description
Server's external address or name	Displays the Faspex Web UI server's primary IP address or domain name. To change it, refer to *asctl Command Reference* on page 165 and use following command: `asctl apache:hostname <host>` Note that <host> should be replaced with the new hostname or IP address.
HTTP port	Displays the Faspex Web UI server's HTTP port number. To change it, refer to *asctl Command Reference* on page 165 and use the following command: `asctl apache:http_port <port>` Note that <port> should be replaced with the new HTTP port number.
HTTPS port	Displays the Faspex Web UI server's secure HTTP (HTTPS) port number. To change it, refer to *asctl Command Reference* on page 165 and use the following command: `asctl apache:https_port <port>` Note that <port> should be replaced with the new HTTPS port number.

Configuration Option	Description
Enable alternate address *checkbox* and *text field*	Enable this checkbox if you have a group of users (for example, those who are external to your organization) that need to access a different IP address or domain name for logging into Faspex (which you will specify in the text field).
Emails include alternate address *checkbox*	When this checkbox is selected, package notifications sent to recipients will include the alternate address, in addition to the primary address.

IMPORTANT NOTE: If you change any of the alternate address configuration options, you must click the **Update** button to apply and save your changes.

> Create an SSL Certificate (Apache)

Generating an RSA Private Key and CSR for your Apache Web Server

Follow the steps below to generate an RSA Private Key, Certificate Signing Request (CSR) and optional self-signed certificate using OpenSSL. For your organization's internal and/or testing purposes, Aspera also provides *server.crt* and *server.key*, which are located in the following directory:

OS Version	File Location
32-bit Windows	C:\Program Files\Common Files\Aspera\Common\apache\conf\
64-bit Windows	C:\Program Files (x86)\Common Files\Aspera\Common\apache\conf\

1. Create a working directory

   In a Command Prompt window (**Start menu** > **All Programs** > **Accessories** > **Command Prompt**), create a new working directory as follows:

```
> cd c:\
> mkdir ssl
> cd c:\ssl
```

2. Copy openssl.cnf to your working directory

   Enter the following commands in your Command Prompt window:

OS Version	Commands
32-bit Windows	`> copy "c:\Program Files\Common Files\Aspera\common\apache\conf\openssl.cnf" "c:\ssl\"` `> cd c:\ssl`
64-bit Windows	`> copy "c:\Program Files (x86)\Common Files\Aspera\common\apache\conf\openssl.cnf" "c:\ssl\"`

OS Version	Commands
	`> cd c:\ssl`

3. Enter the OpenSSL command to generate your Private Key and Certificate Signing Request

   In this step, you will generate an RSA Private Key and CSR using OpenSSL. In a *Command Prompt* window, enter the following command (where **my_key_name.key** is the name of the unique key that you are creating and **my_csr_name.csr** is the name of your CSR):

```
> openssl req -config "c:\ssl\openssl.cnf" -new -nodes -keyout my_key_name.key -
out my_csr_name.csr
```

   Note that in the example above, the *.key* and *.csr* files will be written to the **c:\ssl** directory.

4. Enter your X.509 certificate attributes

   After entering the command in the previous step, you will be prompted to input several pieces of information, which are the certificate's X.509 attributes.

IMPORTANT NOTE: The *common name* field must be filled in with the fully qualified domain name of the server to be protected by SSL. If you are generating a certificate for an organization ***outside of the US***, please refer to the link *http://www.iso.org/iso/english_country_names_and_code_elements* for a list of 2-letter, ISO country codes.

```
Generating a 1024 bit RSA private key
.....................++++++
.................++++++
writing new private key to 'my_key_name.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:Your_2_letter_ISO_country_code
State or Province Name (full name) [Some-State]:Your_State_Province_or_County
Locality Name (eg, city) []:Your_City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Your_Company
Organizational Unit Name (eg, section) []:Your_Department
Common Name (i.e., your server's hostname) []:secure.yourwebsite.com
Email Address []:johndoe@yourwebsite.com
```

You will also be prompted to input "extra" attributes, including an optional *challenge password*. Please note that manually entering a challenge password when starting the server can be problematic in some situations (e.g., when starting the server from the system boot scripts). You can skip inputting a challenge password by hitting the "enter" button.

```
...
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

After finalizing the attributes, the private key and CSR will be saved to your root directory.

IMPORTANT NOTE: If you make a mistake when running the OpenSSL command, you may discard the generated files and run the command again. After successfully generating your key and Certificate Signing Request, be sure to guard your private key, as it cannot be re-generated.

5. Send CSR to your signing authority

You now need to send your unsigned CSR to a Certifying Authority (CA). Once the CSR has been signed, you will have a real Certificate, which can be used by Apache.

IMPORTANT NOTE: Some Certificate Authorities provide a Certificate Signing Request generation tool on their Website. Please check with your CA for additional information.

6. *(Optional)* Generate a Self-Signed Certificate

At this point, you may need to generate a self-signed certificate because:

- You don't plan on having your certificate signed by a CA
- Or you wish to test your new SSL implementation while the CA is signing your certificate

You may also generate a self-signed certificate through OpenSSL. This temporary certificate will generate an error in the client's browser to the effect that the signing certificate authority is unknown and not trusted. To generate a temporary certificate (which is good for 365 days), issue the following command:

```
openssl x509 -req -days 365 -in my_csr_name.csr -signkey my_key_name.key -
out my_cert_name.crt
```

7. Copy Key and Certificate into target directory

After receiving your signed certificate from your CA, copy the files into Apache's */conf* directory and edit your ***httpd-ssl.conf*** file (note that you can store the certificate and key in any directory, as long as the path(s) are updated in your configuration file. For additional information, please continue to the topic *Create an SSL Certificate (Apache)*.

> Enable SSL (Apache)

Set up an SSL certificate for your *Faspex Server* Web UI.

To enable an SSL certificate for your *Faspex Server* Web UI, follow the steps below. Note that these instructions assume that you have already created your certificate and key files as instructed in the topic *Create an SSL Certificate (Apache)*.

1. Verify/update Apache's SSL configuration file and save

   You will find your Apache SSL configuration file in the following location:

OS Version	File
32-bit Windows	C:\Program Files\Common Files\Aspera\Common\apache\conf\extra\httpd-ssl.conf
64-bit Windows	C:\Program Files (x86)\Common Files\Aspera\Common\apache\conf\extra\httpd-ssl.conf

   Update the *SSLCertificateFile* and *SSLCertificateKeyFile* information within *httpd-ssl.conf* so that it corresponds with the certificate path(s) and file name(s) that you have created or are currently using. For example:

```
...
SSLCertificateFile     /path/to/my_cert_name.crt
SSLCertificateKeyFile  /path/to/my_key_name.key
...
```

   Note that *SSLCertificateFile* and *SSLCertificateFile* have been provided in the "`/conf`" directory for testing purposes.

2. Restart your Apache Web Server and test your SSL connection

   Restart Apache using the following command:

```
asctl apache:restart
```

   Then, go to the `https://<your-server-ip-or-name>/aspera/faspex` to test your SSL setup. **Note that this must be the same hostname that you entered into the *common name* field when creating your certificate.** For details, please refer to *Create an SSL Certificate (Apache)*.

> Regenerate Self-Signed SSL Certificate (Apache)

Update your existing Faspex, self-signed SSL certificate.

When Faspex is initially set up on your system, a pre-generated, self-signed SSL certificate is also installed. If you have changed your Apache hostname, you will need to regenerate the self-signed certificate by following the instructions below.

1. Open a *Command Prompt* window and run the *asctl* command

   In a Command Prompt window (**Start menu** > **All Programs** > **Accessories** > **Command Prompt**), run the following command to generate a new, self-signed SSL certificate for your installation of Faspex (where you will replace the HOSTNAME with your Apache server's IP address or host name):

   ```
   > asctl apache:make_ssl_cert HOSTNAME
   ```

   Note that you will need to answer **yes** when prompted to overwrite the existing certificate.

2. Confirm that your certificates have been updated

   Check the following location to confirm whether or not your self-signed SSL certificates have been updated:

OS Version	File
32-bit Windows	• C:\Program Files\Common Files\Aspera\Common\apache\conf\server.crt • C:\Program Files\Common Files\Aspera\Common\apache\conf\server.key
64-bit Windows	• C:\Program Files (x86)\Common Files\Aspera\Common\apache\conf\server.crt • C:\Program Files (x86)\Common Files\Aspera\Common\apache\conf\server.key

Transfer Server

Configure Faspex to communicate with a transfer node.

Before configuring Faspex to communicate with a remote transfer server, it is important to understand how it is able to do so. Enterprise (or Connect) Server v3.0+ features the Node API, a daemon that offers REST-inspired file operations and a transfer management API. When you install Enterprise (or Connect) Server 3.0+ on a local/remote system or EC2 instance, it becomes an Aspera "node." Faspex can be installed on the transfer node, *or* it can access the transfer node remotely via the Node API. This topic explains how to configure Faspex to access a remote transfer node and directory shares.

First, make sure that you have Enterprise (or Connect) Server 3.0+ installed on the remote machine, and have followed the steps in "*Setting up a Remote Server*" to prepare the machine. To continue, make sure you have the following information at hand:

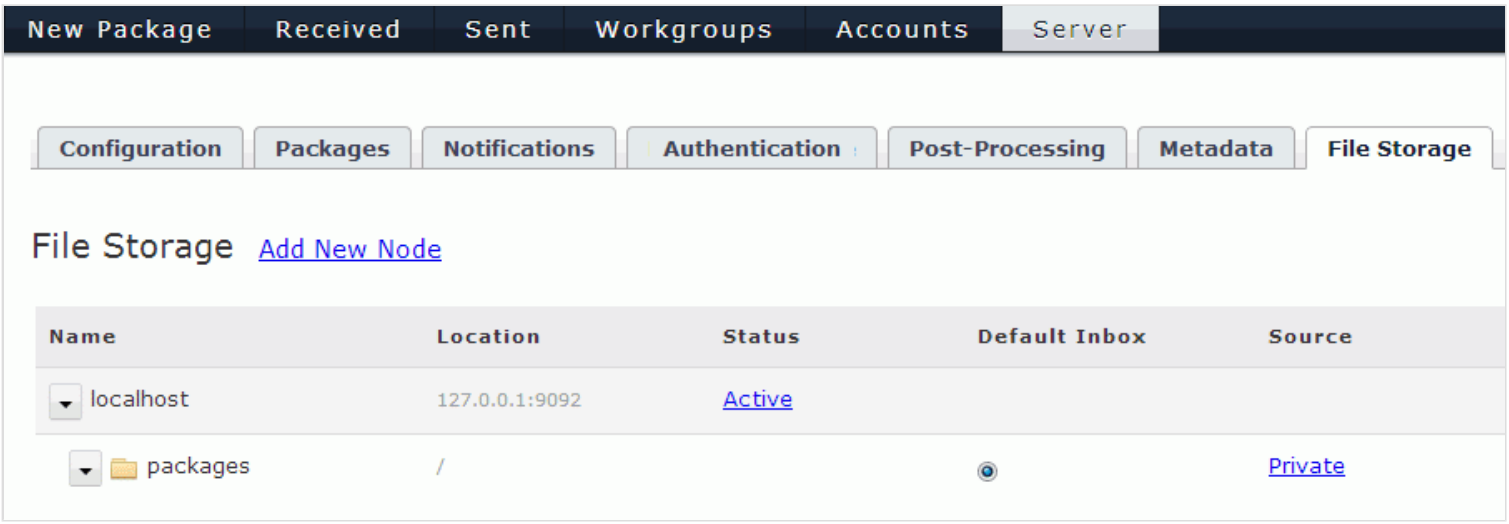
- The node computer's hostname or IP address, along with a port and path (if applicable).

- The node API username and password, which you created when you set up Enterprise Server on your node machine.

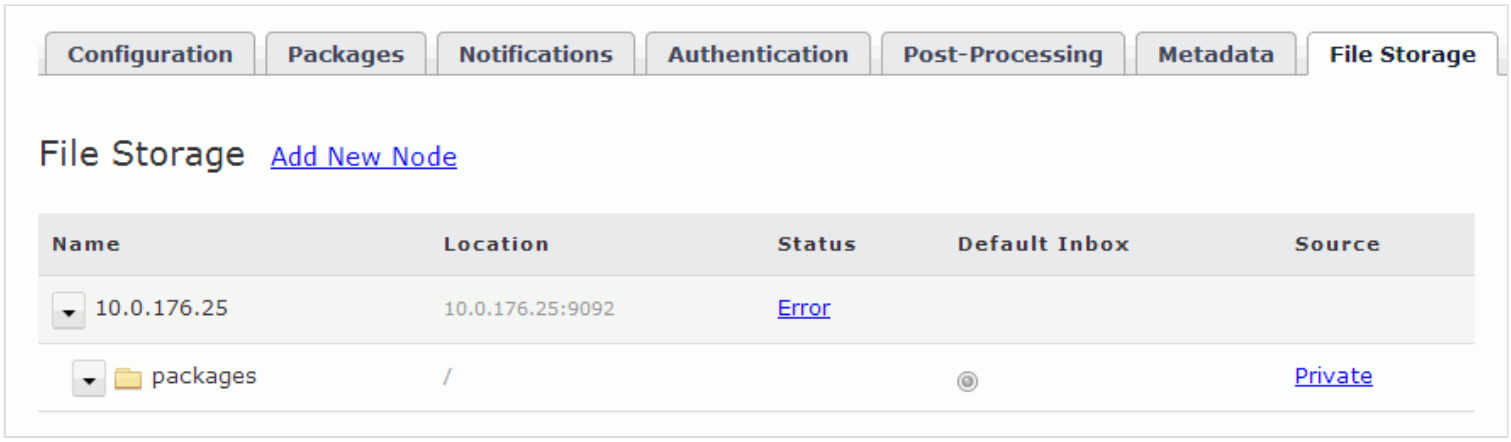
If you do not have this information, please refer to the admin guide for Enterprise Server or Connect Server v3.0+.

Transfer Server Configuration Screen

From the Faspex web UI, go to **Server** > **File Storage** to configure access to the node that manages your Aspera transfers. If Faspex was installed with the *streamlined* option, your transfer server (the node where Enteprise or Connect Server is installed) is configured by default as being on the same machine as your Faspex Web server (by default, 127.0.0.1). When you initially view the **File Storage** page, you will find that the IP address or domain name is the same as that of your Web server, as shown below. On a fresh install, the default Faspex transfer server, `localhost`, is the only server listed on the File Storage page, and its default storage directory, `packages`, is shown as the default inbox destination.

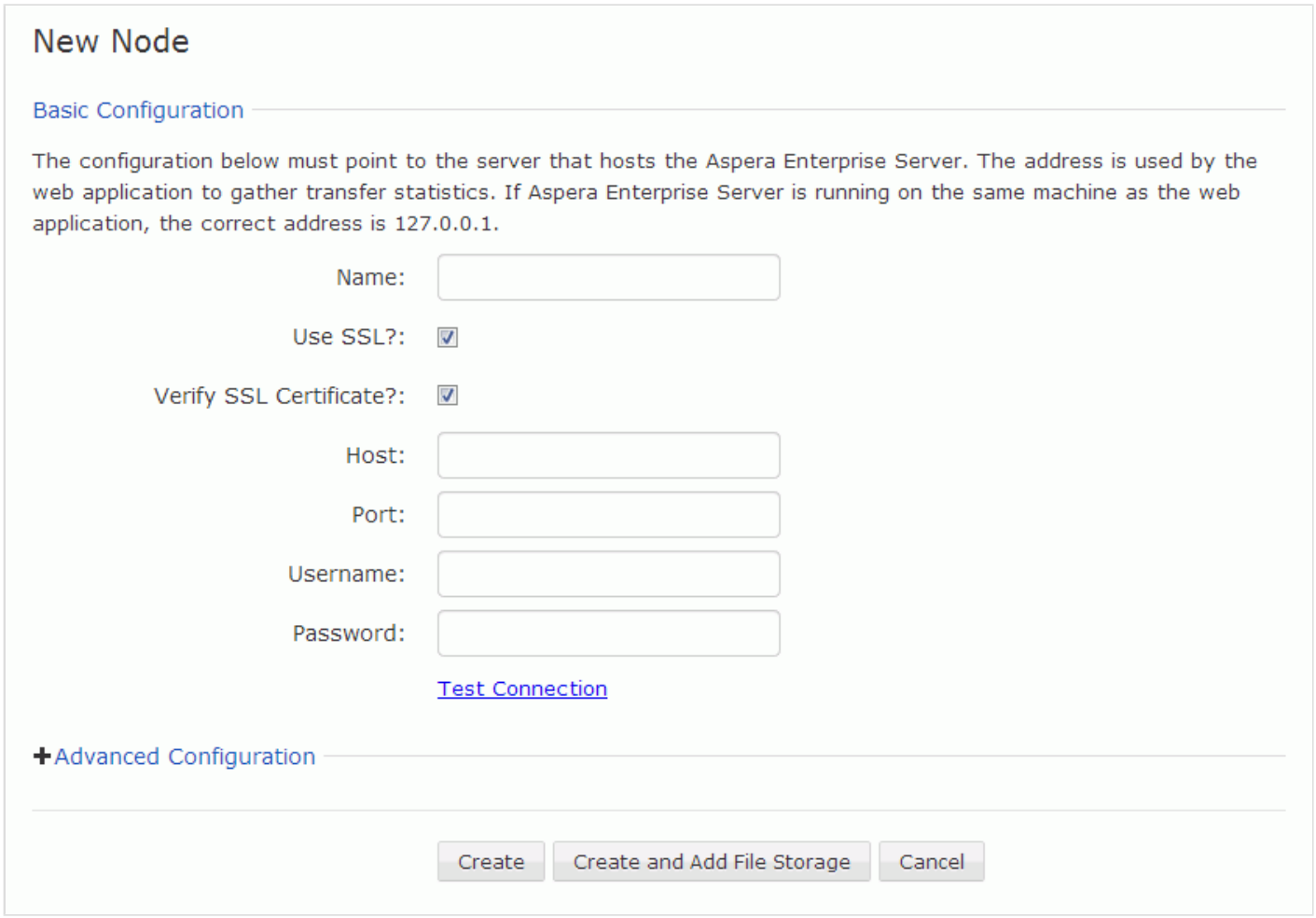


If Faspex was installed with the *detailed* option, your transfer server (the node where Enteprise or Connect Server is installed) is configured to be a remote server. When you initially view the **File Storage** page, you will find that the IP address or domain name is that of your remote server, as shown below. On a fresh install, the remote Faspex transfer server is the only server listed on the File Storage page. In this case, the default storage directory, `packages`, will not be functional until valid node admin credentials (empty by default) are entered for the remote server.



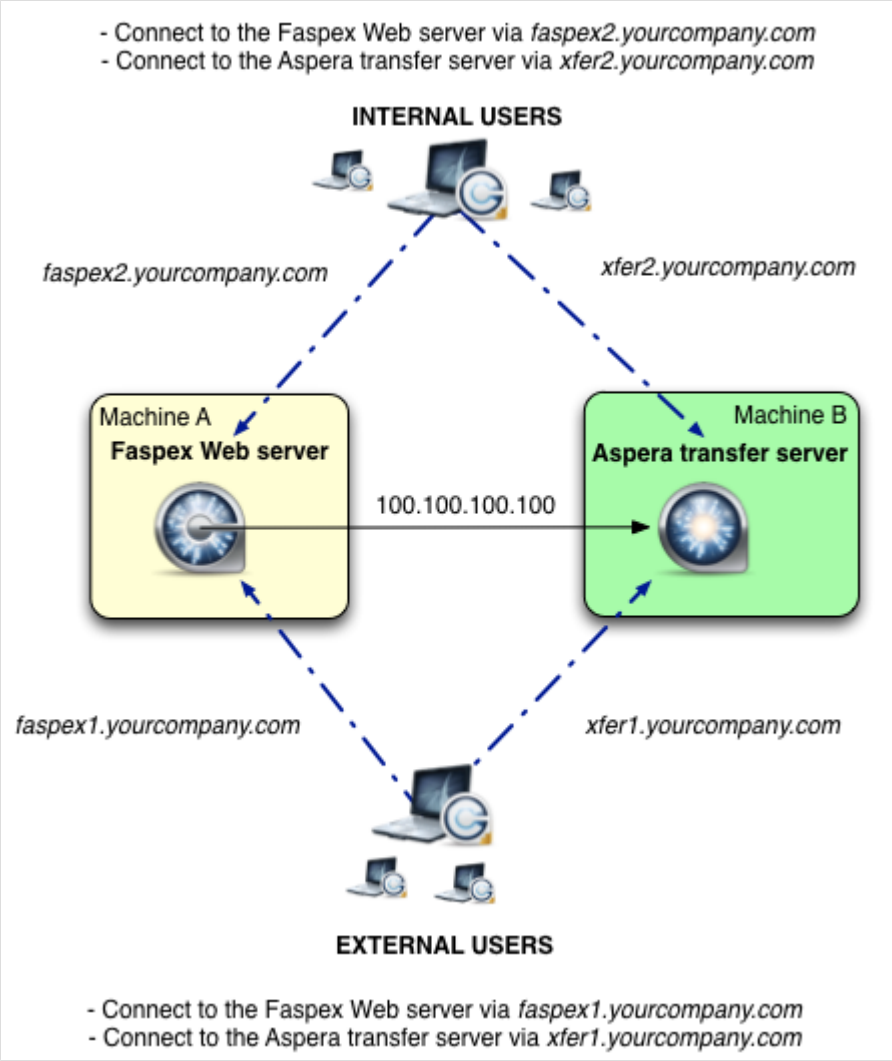
In the above display, you will also see a summary of sources (from where files are sent) and inboxes (where received files are stored). For details on inboxes and file storage, see *File Storage* on page 99.

To configure a different machine as your transfer server, click the **Add New Node** link, which takes you to the New Node configuration screen:

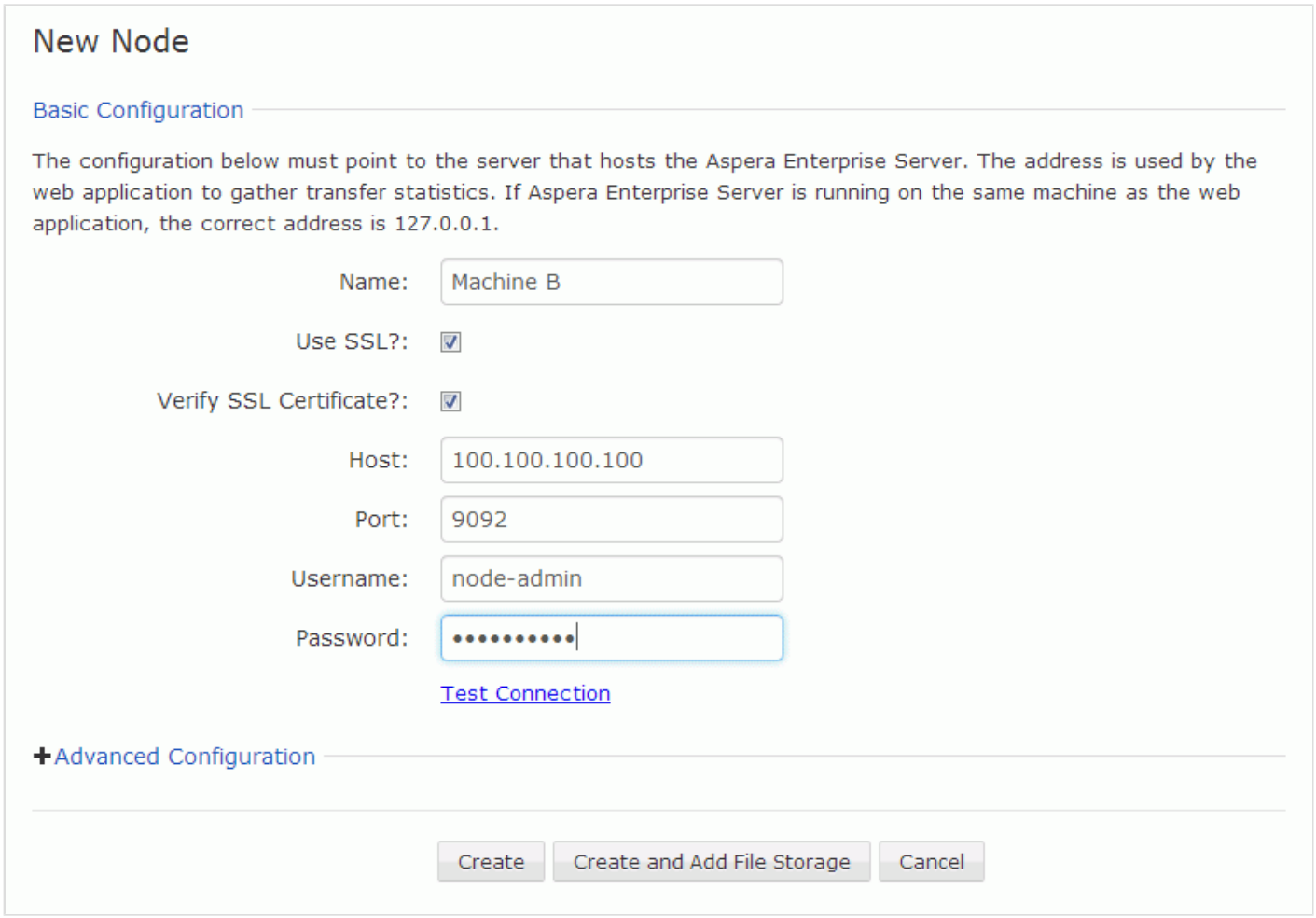


Transfer Server Address for the Web Server

For a *streamlined* installation, your transfer server address, by default, is `127.0.0.1`, because Faspex is installed on the same machine as your transfer server (i.e., Enterprise or Connect Server v3.0+). To run your transfer server on a different machine, you need to tell the Faspex web server where that machine is located so that Faspex can gather transfer statistics and display them via the Web UI. Consider the configuration in the following example:



In the image below, the New Node screen has been filled in for the above configuration:



Field	Description	Sample Value
Name	Unique name to identify the remote node.	"Machine B"
Use SSL	To encrypt the connection to the node using SSL, enable this box. For details, see *> Setting up SSL for Faspex Nodes* on page 50.	Enabled, by default.
Verify SSL Certificate	To verify the SSL certificate, enable this box.	Enabled, by default.
Host	The node's hostname or IP address. CAUTION: To avoid connectivity problems, do not specify a hostname that contains underscores.	In this example, Faspex can access the transfer node at "100.100.100.100". (Depending on your setup, this value could be different.)
Port	The node's port number.	HTTPS 9092. (Depending on your setup, this value could be different.)

Field	Description	Sample Value
Username	The node API username that was created when Enterprise (or Connect) Server 3.0+ was set up on the node machine.	"node-admin"
Password	The node API password that was created when Enterprise (or Connect) Server 3.0+ was set up on the node machine.	"`s3cur3_p433`"

Once you have entered this information, you can test the node connection by clicking the **Test Connection** link. If you have a group of users that needs to use a different transfer address (as in the example configuration above), this can be set in the Advanced Configuration area as described in the next section. Otherwise, at this point, you can click **Create** to add the transfer server node to your Faspex configuration. For information about adding file storage to this node, see *File Storage* on page 99.

IMPORTANT NOTE: To use *HTTP or HTTPS Fallback* for a transfer server on a separate (remote) machine, you must configure your transfer server and firewall ports in *one* of the following ways:

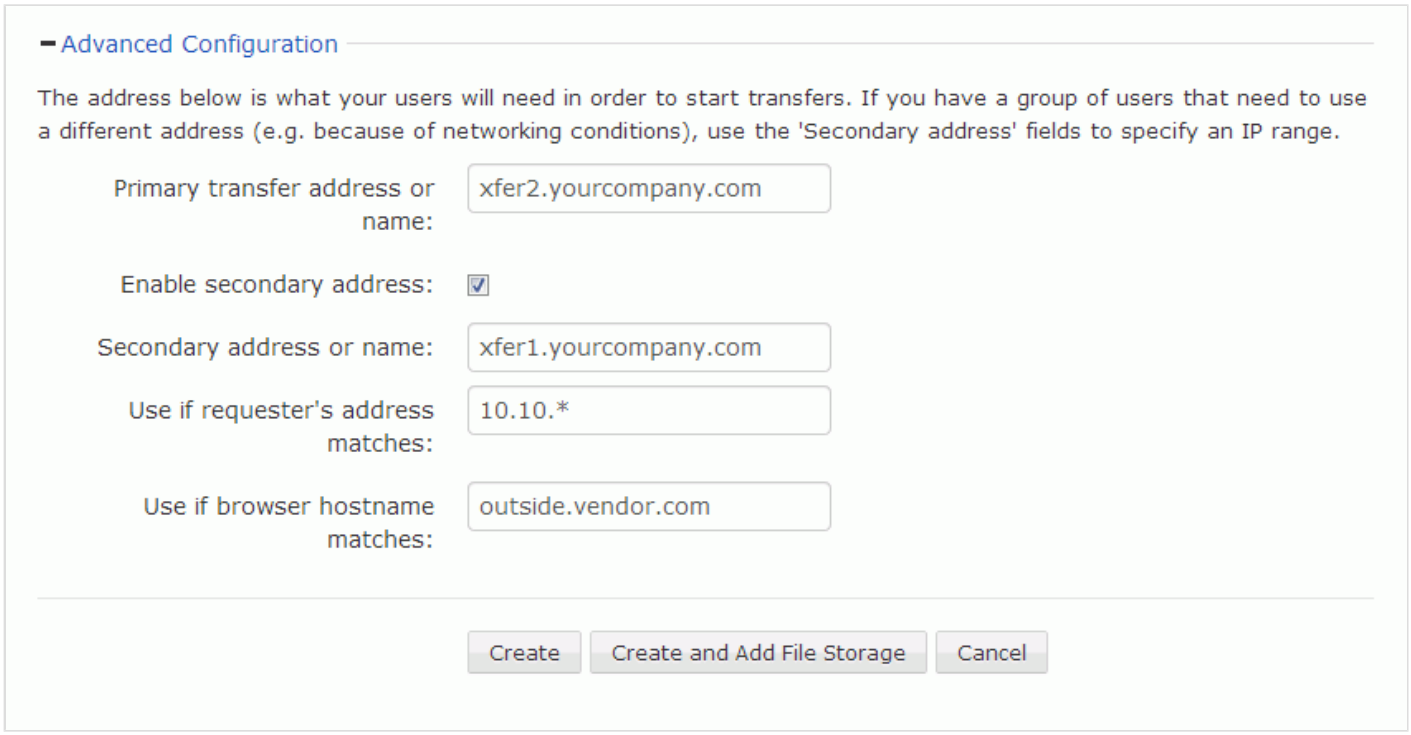
- HTTP/HTTPS enabled and set to defaults (8080 + 8443) *AND* firewall port open on 8080/8443.
- HTTP/HTTPS enabled and set to standard ports (80 + 443) *AND* firewall port open on 80/443.

Additionally, the transfer server's fallback settings *must match* Faspex's fallback settings; otherwise, Faspex will return a "Package creation failed" error. This includes ensuring that the transfer server has HTTP/HTTPS fallback enabled; and that (within the Web GUI) Faspex has **Server** > **Configuration** > **Transfer Options** > **Enable HTTP Fallback** and **Server** > **Configuration** > **Security** > **Encrypt Transfers** (for HTTPS fallback) turned on. For security, Aspera highly recommends using HTTPS fallback. If HTTPS fallback is enabled on the transfer server, then encrypted transfers must be enabled in the Faspex Web GUI.

Transfer Server Address for Users

In the example configuration above, the Aspera transfer server is accessible by different host names for both internal and external users. Thus, we can complete the "Advanced Configuration" section as follows:

- Your Web server communicates with the transfer node using `100.100.100.100`.
- Your internal users communicate with the transfer node using `xfer2.yourcompany.com`.
- Your external users communicate with the transfer node using `xfer1.yourcompany.com`. In addition to specifying a secondary address/name, you can also set conditions for when the secondary address is to be used (e.g., if the requester's IP address matches `X.X.X.X` or the browser hostname matches `outside.vendor.com`).



Field	Description	Sample Value
Primary transfer address or name:	IP address or host name your users will need in order to start transfers, if different from the *Host* address or name specified in *Basic Configuration*. If the host IP address for the transfer server is 127.0.0.1--that is, the node is on the same machine as the web application--users will need the external address of the node, which you would specify here.	"`xfer2.yourcompany.com`"
Enable secondary address:	Check this box if you have a group of external users who must access the transfer node through a secondary IP address or domain name.	Disabled, by default.
Secondary address or name:	The secondary address or name.	"`xfer1.yourcompany.com`"
Use if requester's address matches:	Set a condition that the requester's IP address must match this range for the secondary transfer address to be used. The value can be a partial string with wild cards; e.g., 10.0.176.*.	"`10.10.*`"
Use if browser hostname matches:	Set a condition that the requested browser hostname or IP address must match this value for the secondary transfer address to be used. For an IP address, the value can be a range of addresses; e.g., 10.0.176.*.	"`outside.vendor.com`"

> Setting up SSL for Faspex Nodes

Setting up SSL for your remote transfer server.

By default, your transfer server address is `127.0.0.1` because Faspex assumes that it is installed on the same machine as your Aspera transfer server (i.e. Enterprise or Connect Server v3.0+). If you are running your transfer server on a different/remote machine (using the Aspera Node API), you can encrypt the connection between the Faspex Web server and the node using SSL. The transfer node is configured to use Aspera's pre-installed, self-signed certificate (`aspera_server_cert.pem`), which is located in the following directory:

- *(Windows 32-bit)* C:\Program Files\Aspera\Enterprise Server\etc
- *(Windows 64-bit)* C:\Program Files (x86)\Aspera\Enterprise Server\etc

Perform the steps below to set up your Faspex and remote transfer server nodes for HTTPS communication.

ABOUT PEM FILES: The PEM certificate format is commonly issued by Certificate Authorities. PEM certificates have extensions that include .pem, .crt, .cer, and .key, and are Base-64 encoded ASCII files containing "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format.

IMPORTANT NOTE: Before proceeding, launch the Faspex Web GUI and go to **Server** > **Configuration** > **Transfer Server** . Here, confirm that **Use SSL** is enabled (which should be, by default). If you are using a *valid, signed* certificate, then enable **Verify SSL Certificate** as well. You do not need to enable **Verify SSL Certificate** if you are testing a *self-signed* certificate.

1. Test your connection to the transfer node using Faspex's sample `cert.pem` file.

   On your Faspex machine, go to the following directory to copy Aspera's `cert.pem.sample` file:

   - *(Windows 32-bit)* C:\Program Files\Aspera\Faspex\config\
   - *(Windows 64-bit)* C:\Program Files (x86)\Aspera\Faspex\config\

   Place a copy of the sample file in the `/ssl` directory (shown below) and remove the `.sample` suffix.

   - *(Windows 32-bit)* C:\Program Files\Aspera\Faspex\config\ssl\
   - *(Windows 64-bit)* C:\Program Files (x86)\Aspera\Faspex\config\ssl\

IMPORTANT NOTE: Your `cert.pem` file should contain the list of CA Root Certificates in PEM format. Please refer to the sample `cert.pem` file as a reference.

   To verify this setup, create a Faspex package and confirm that your remote transfer server is able to send the package to another user.

Continue to the next step if you would like to create your own SSL Certificate (to either self-sign, or send to a signing authority).

2. Create a working directory

   In a Command Prompt window (**Start menu** > **All Programs** > **Accessories** > **Command Prompt**), create a new working directory as follows:

```
> cd c:\
> mkdir ssl
> cd c:\ssl
```

3. Copy openssl.cnf to your working directory

   Enter the following commands in your Command Prompt window:

OS Version	Commands
32-bit Windows	`> copy "c:\Program Files\Common Files\Aspera\common\apache\conf\openssl.cnf" "c:\ssl\"` `> cd c:\ssl`
64-bit Windows	`> copy "c:\Program Files (x86)\Common Files\Aspera\common\apache\conf\openssl.cnf" "c:\ssl\"` `> cd c:\ssl`

4. Enter the OpenSSL command to generate your Private Key and Certificate Signing Request

   In this step, you will generate an RSA Private Key and CSR using OpenSSL. In a *Command Prompt* window, enter the following command (where **my_key_name.key** is the name of the unique key that you are creating and **my_csr_name.csr** is the name of your CSR):

```
> openssl req -config "c:\ssl\openssl.cnf" -new -nodes -keyout my_key_name.key -out my_csr_name.csr
```

   Note that in the example above, the *.key* and *.csr* files will be written to the **c:\ssl** directory.

5. Enter your X.509 certificate attributes

   After entering the command in the previous step, you will be prompted to input several pieces of information, which are the certificate's X.509 attributes.

IMPORTANT NOTE: The *common name* field must be filled in with the fully qualified domain name of the server to be protected by SSL. If you are generating a certificate for an organization ***outside of the US***, please refer to the link *http://www.iso.org/iso/english_country_names_and_code_elements* for a list of 2-letter, ISO country codes.

```
Generating a 1024 bit RSA private key
.....................++++++
.................++++++
writing new private key to 'my_key_name.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:Your_2_letter_ISO_country_code
State or Province Name (full name) [Some-State]:Your_State_Province_or_County
Locality Name (eg, city) []:Your_City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Your_Company
Organizational Unit Name (eg, section) []:Your_Department
Common Name (i.e., your server's hostname) []:secure.yourwebsite.com
Email Address []:johndoe@yourwebsite.com
```

You will also be prompted to input "extra" attributes, including an optional *challenge password*. Please note that manually entering a challenge password when starting the server can be problematic in some situations (e.g., when starting the server from the system boot scripts). You can skip inputting a challenge password by hitting the "enter" button.

```
...
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

After finalizing the attributes, the private key and CSR will be saved to your root directory.

IMPORTANT NOTE: If you make a mistake when running the OpenSSL command, you may discard the generated files and run the command again. After successfully generating your key and Certificate Signing Request, be sure to guard your private key, as it cannot be re-generated.

6. Send CSR to your signing authority

   You now need to send your unsigned CSR to a Certifying Authority (CA). Once completed, you will have valid, signed certificate.

IMPORTANT NOTE: Some Certificate Authorities provide a Certificate Signing Request generation tool on their Website. Please check with your CA for additional information.

7. *(Optional)* Generate a Self-Signed Certificate.

   At this point, you may need to generate a self-signed certificate because:

   - You don't plan on having your certificate signed by a CA
   - Or you wish to test your new SSL implementation while the CA is signing your certificate

   You may also generate a self-signed certificate through OpenSSL. To generate a temporary certificate (which is good for 365 days), issue the following command:

   ```
   openssl x509 -req -days 365 -in my_csr_name.csr -signkey my_key_name.key -
   out my_cert_name.crt
   ```

8. Create the PEM file.

   After generating a new certificate, you must create a `cert.pem` file that contains both the private key and the certificate. To do so, copy and paste the entire body of the key and cert files into a single text file and save the file as `cert.pem`. Lastly, place a copy of the `cert.pem` file in Faspex's `config/ssl` directory (shown below).

   - *(Windows 32-bit)* C:\Program Files\Aspera\Faspex\config\ssl\
   - *(Windows 64-bit)* C:\Program Files (x86)\Aspera\Faspex\config\ssl\

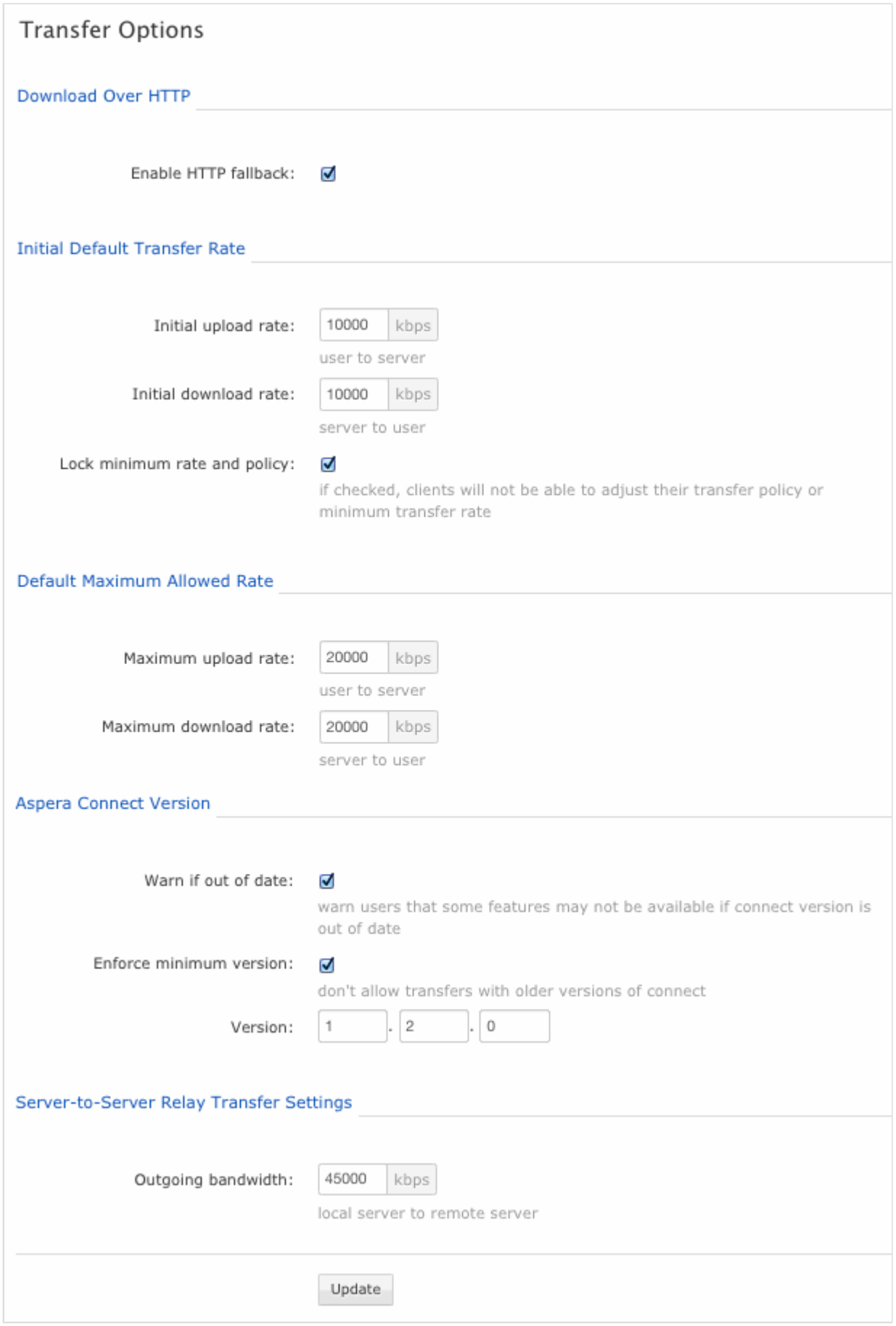
IMPORTANT NOTE: Your `cert.pem` file should contain the list of CA Root Certificates in PEM format. Please refer to the sample `cert.pem` (*described in Step 1, above*) as a reference.

   To verify this setup, create a Faspex package and confirm that your remote transfer server is able to send the package to another user.

Transfer Options

Configure your Faspex Server's transfer settings.

Within the Faspex Server Web UI, go to **Server** > **Configuration** > **Transfer Options** to view and/or modify your server's transfer settings, including HTTP fallback, default transfer rates, Aspera Connect browser plugin behavior and server-to-server relay outgoing bandwidth.


Transfer Options
Download Over HTTP
Enable HTTP fallback:
Initial Default Transfer Rate
Initial upload rate:
10000
kbps
user to server
Initial download rate:
10000
kbps
server to user
Lock minimum rate and policy:
if checked, clients will not be able to adjust their transfer policy or minimum transfer rate
Default Maximum Allowed Rate
Maximum upload rate:
20000
kbps
user to server
Maximum download rate:
20000
kbps
server to user
Aspera Connect Version
Warn if out of date:
warn users that some features may not be available if connect version is out of date
Enforce minimum version:
don't allow transfers with older versions of connect
Version:
1
2
0
Server-to-Server Relay Transfer Settings
Outgoing bandwidth:
45000
kbps
local server to remote server
Update

Download Over HTTP

Configuration Option	Description
Enable HTTP fallback	Enable or disable the HTTP fallback feature, which provides a secondary transfer method for users whose UDP connection is lost or cannot be established. When HTTP fallback is enabled, the transfer will be continued over the HTTP protocol (or, if transfer encryption is enabled, over the HTTPS protocol). For additional information on configuring HTTP fallback, please refer to *Configuring HTTP and HTTPS Fallback* on page 138.

Initial Default Transfer Rate

Configuration Option	Description
Inital upload rate	The default *fasp* transfer upload speed in kbps (i.e. user to server)
Initial download rate	The default *fasp* transfer download speed in kbps (i.e. server to user)
Lock minimum rate and policy *(checkbox)*	When enabled, users will be unable to adjust their transfer policy or minimum transfer rate.

Default Maximum Allowed Rate

Configuration Option	Description
Maximum upload rate	The maximum *fasp* transfer upload speed in kpbs (i.e. user to server)
Maximum download rate	The maximum *fasp* transfer download speed in kbps (i.e. server to user)

Aspera Connect Version

Configuration Option	Description
Warn if out of date *(checkbox)*	When enabled, users will be warned when their Aspera Connect browser plugin is out-of-date.
Enforce minimum version *(checkbox)*	When enabled, users with a deprecated version of Aspera Connect will not be allowed to perform transfers (i.e., send and receive packages).
Version	Specify the minimum accepted version of Aspera Connect.

Server-to-Server Relay Transfer Settings

Configuration Option	Description
Outgoing bandwidth	If you have more than one Faspex server in your organization and are utilizing server-to-server relay, then you may specify the transfer bandwidth between servers.

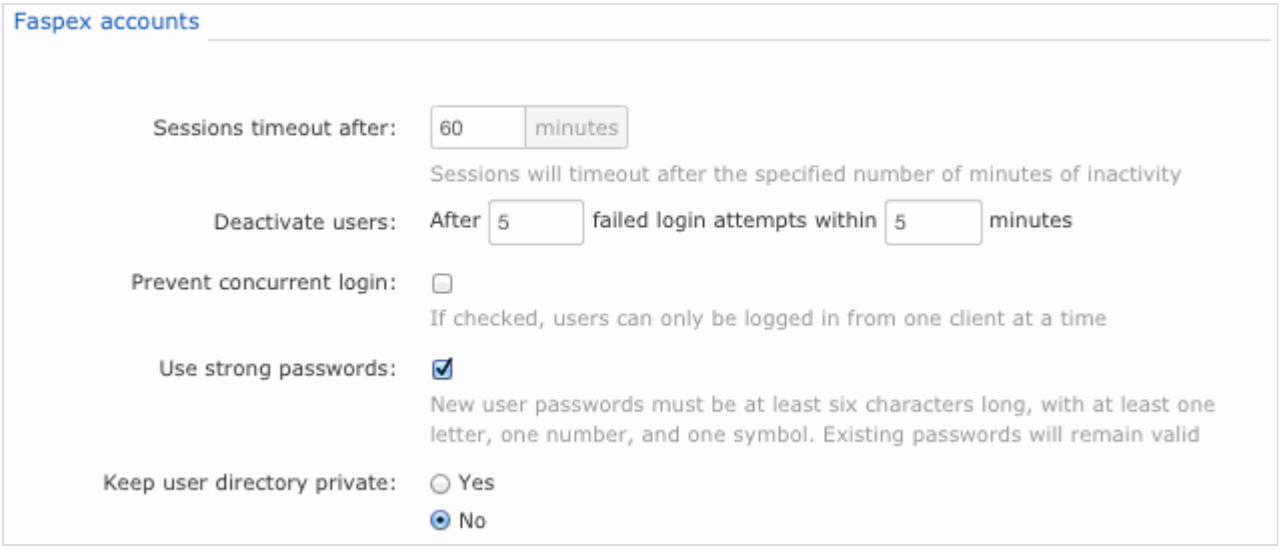
IMPORTANT NOTE: You must click the **Update** button to apply and save your changes.

Security

Configure your Faspex Server's security settings.

Within the Faspex Server Web UI, go to **Server** > **Configuration** > **Security** to view and/or modify your server's security settings for Faspex user accounts, self registration, external senders and encryption.

Faspex Accounts



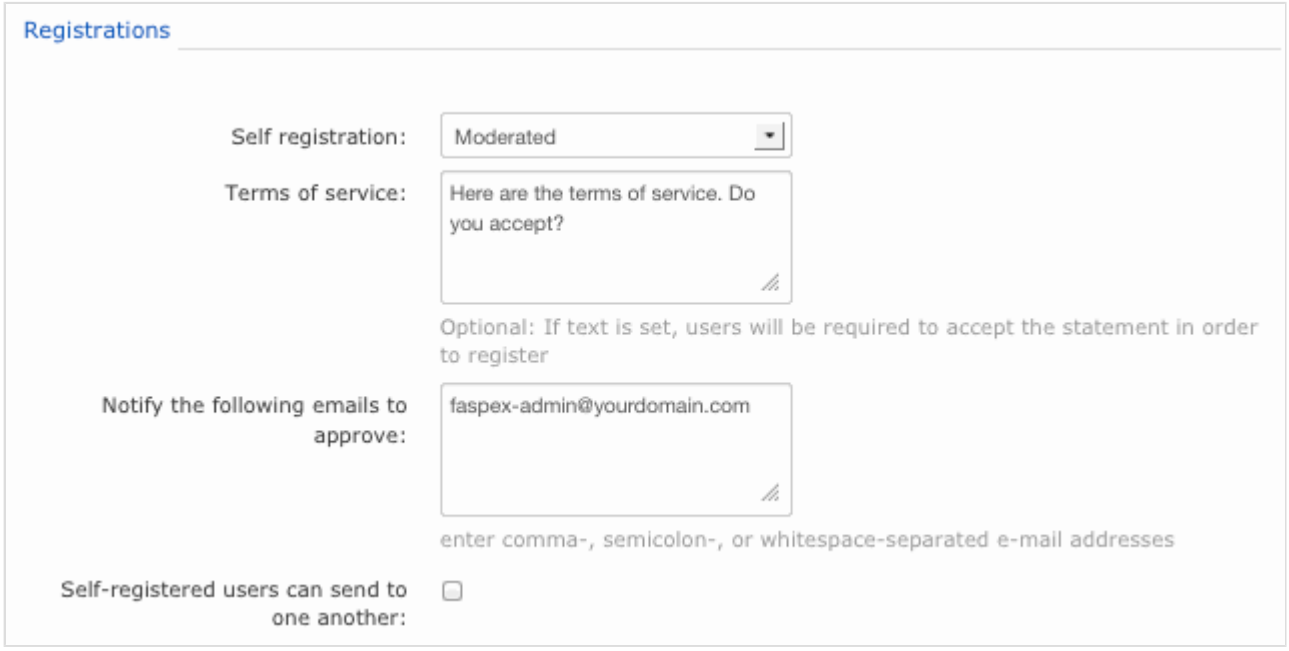
Configuration Option	Description
Session timeout	Sessions will time out after the specified number of minutes of inactivity.
Deactivate users	Deactivate the user account when login attempts fail under the specified circumstance. Note that deactivated Directory Service (DS) users will be reactivated on a subsequent sync with the DS server.
Prevent concurrent login *(checkbox)*	If enabled, users can only be logged in from one client at a time.
Use strong passwords *(checkbox)*	If enabled, requires newly created passwords to contain at least one letter, one number and one symbol. Note that existing passwords will remain valid. Administrators may

Configuration Option	Description

	also change the strong password criteria by editing the *faspex.yml* file, which is located in the following directory:
	• **(Windows 32-bit)** `C:\Program Files\Aspera\Faspex\config\faspex.yml`
	• **(Windows 64-bit)** `C:\Program Files (x86)\Aspera\Faspex\config\faspex.yml`
	
	Inside *faspex.yml*, paste the following (where `StrongPasswordRegex` is the password criteria as a regular expression and `StrongPasswordRequirements` is the description that appears to the user underneath the field):
	
	`StrongPasswordRegex: (?=.*[A-Z])(?=.*(\d|\W|_)).{7,}`
	`StrongPasswordRequirements: "Password must meet this criteria..."`

Keep user directory private *(Yes/No)*	When set to **Yes**, prevents a Faspex user (even if they have permissions to send to all Faspex users) from being able to see the entire user directory. You can override this setting on a user-by-user basis by editing their permissions. **IMPORTANT NOTE:** When the privacy setting is turned on (set to **Yes**), users who have been assigned the role of **Workgroup Admin** can still view the entire list of Faspex users via the **Workgroup Members** page.

Registrations

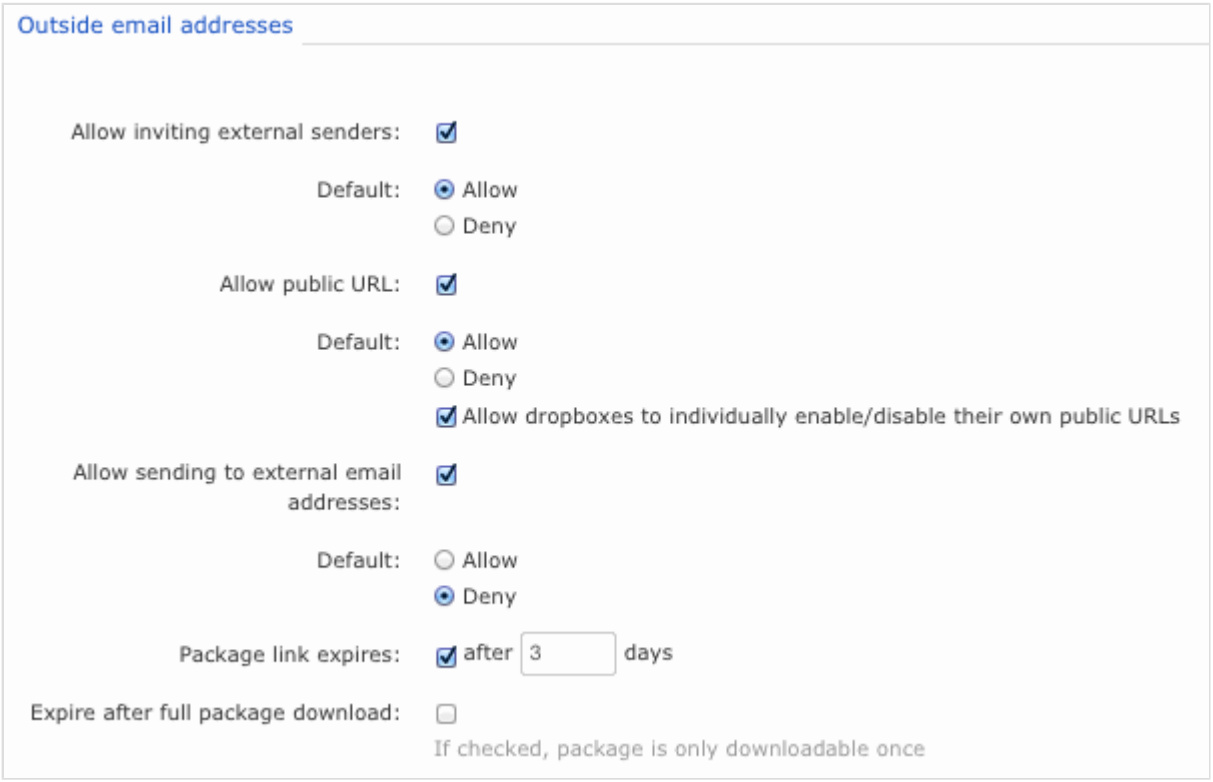


Configuration Option	Description
Self registration	Determines if non-users can create or request user accounts. Choose between **none** (not allowed), **moderated** (an administrator must approve the account before it is created), and **unmoderated** (once a user registers, his or her account will be automatically created). If you allow self-registration, the **moderated** setting is recommeded for security. **SECURITY WARNING:** If self-registration is enabled, then it could be utilized to find out whether a certain account exists on the server. That is, if you attempt to self-register a duplicate account, then you will receive a prompt stating that the user already exists. After a user self-registers (either moderated or unmoderated), his or her account will inherit the permissions of the configured template user and will automatically become members of designated workgroup(s). To configure the template user, go to **Accounts** > **Pending Registrations** > **template user** . To set the workgroups that newly created users will join, click the **workgroups** link. Although self-registered users are not allowed to send packages to other self-registered users, by default, you can modify this setting by checkmarking the **Self-registered users can send to one another** checkbox. **IMPORTANT NOTE:** To prevent a self-registered account from having the same email address as a full Faspex user, Administrators can add a special option to *faspex.yml*. You will find *faspex.yml* in the following directory: • **(Windows 32-bit)** `C:\Program Files\Aspera\Faspex\config\faspex.yml` • **(Windows 64-bit)** `C:\Program Files (x86)\Aspera\Faspex\config\faspex.yml` Inside *faspex.yml*, within the "Production:" section, paste the following option and set it to `true`: `EnforceSelfRegisteredUserEmailUniqueness: true`
Terms of service	*(Optional)* If text is set, then users will be required to accept the statement in order to create an account.
Notify the following emails to approve	This field appears when **moderated** is selected, above. Input one or more email addresses to notify for moderation. Note that these email addresses are not validated against existing Faspex administrators and/or managers.

Configuration Option	Description
Self-registered users can send to one another	When checked, self-registered users will be allowed to send packages to other self-registered users.

MODERATED SELF-REGISTRATION NOTE: If users are allowed to self-register, then they will see a **Request an account** link on the login page. After a user clicks this link and completes the form, then you (as the administrator) will be prompted under **Accounts** > **Pending Registrations** > **Actions** to **Approve** or **Deny** his or her account.

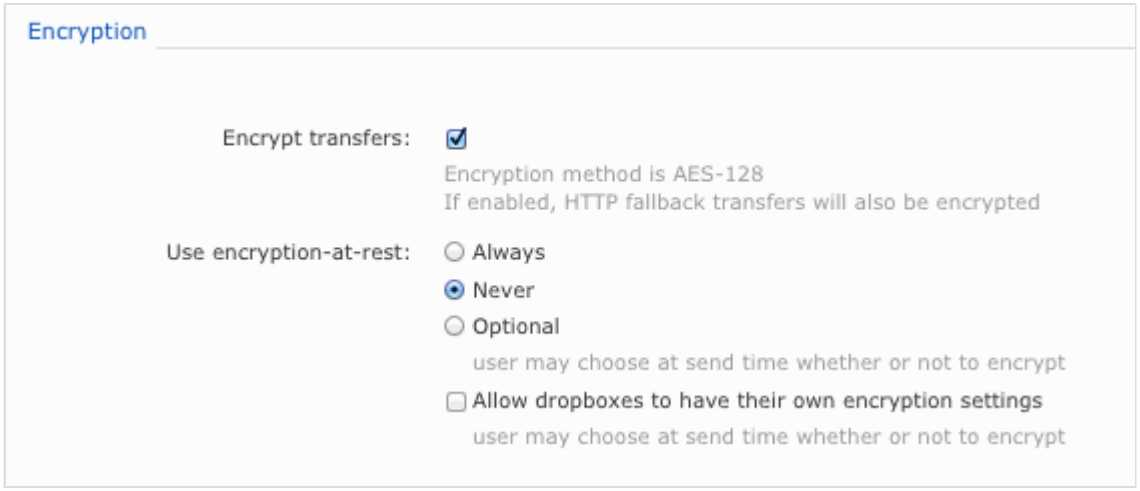
Outside email addresses



Configuration Option	Description
Allow inviting external senders *(checkbox)*	When enabled, external senders (those who do not have Faspex accounts) can be invited to send a package. An Administrator can enable/disable this feature for specific users from the **Accounts** > **[Username]** page, while still retaining the server-wide setting of enabled or disabled. Please refer to *Create a New Faspex User* for details on this user setting.
Allow public URL	A Public URL can be used by external senders to submit packages to both registered Faspex users and dropboxes. The benefit of using a Public URL is in the time-savings, such that external senders no longer need to be individually invited to submit a package

Configuration Option	Description
	(although that functionality still exists). When a Public URL is enabled and posted to a an email, instant message, website, etc., the following workflow occurs: **1. The external sender clicks the Public URL (which could be for either a dropbox or a registered Faspex user).** **2. The sender is directed to page where he or she is asked to enter and submit an email address.** **3. A private link is *automatically* emailed to the sender.** **4. The sender clicks the private link and is automatically redirected to a dropbox or Faspex-user package submission page.** **5. Once the package is submitted through the private link, the dropbox or Faspex user receives it.** Thus, when the field **Allow public URL** is enabled (e.g. set to `Allow`), the Public URL feature is turned on for all Faspex dropboxes and registered users. If the **Allow dropboxes to individually enable/disable their own public URLs** checkbox is enabled as well, then individual dropboxes can override the server setting and turn off this feature. Individual Faspex users, on the other hand, can override the Public URL server setting for their own accounts by going to **Preferences** > **Misc** > **Enable public URL** and disabling the checkbox. **IMPORTANT NOTE:** An Administrator can enable/disable the Public URL feature for specific users from the **Accounts** > **[Username]** page, while still retaining the server-wide setting of enabled or disabled. Please refer to *Create a New Faspex User* for details on this user setting.
Allow sending to external email addresses *(checkbox)*	Faspex packages can be sent to people who do not have Faspex accounts. When set to `Allow`, all Faspex users will be able to send to external email addresses, by default. When set to `Deny`, you must enable this behavior within each individual user account (by checking the option for *Sending to external email* in their account settings). Please refer to *Create a New Faspex User* for details on this user setting.
Package link expires *(checkbox and text field)*	When enabled, the package link will expire after the specified number of days.
Expire after full package download *(checkbox)*	If this checkbox is enabled, the package link will expire after one (1) download (which applies when the link is forwarded, as well). After the first download, the file(s) must be resent in a new package--via the Faspex Server--for the recipient to be able to download them again.

Encryption



Configuration Option	Description
Encrypt transfers *(checkbox)*	Enable this checkbox to encrypt your transfers (AES-128). If enabled, HTTP fallback transfers will also be encrypted.
Use Encryption-at-Rest (EAR) *(radio buttons and checkbox)*	• **Always:** Always use EAR. When enabled, users will be required, on upload, to enter a password to encrypt the files on the server. Subsequently, recipients will be required to enter the password to decrypt protected files as they are being downloaded. Note that if a user elects to keep downloaded files encrypted, then they do not need to enter a password until they attempt to decrypt the files locally. **This feature is not fully enforced unless the Faspex Server Administrator also updates the aspera.conf configuration file (which is not automatically modified by Faspex).** The Administrator may update *aspera.conf* manually, as well as using the Aspera Enterprise Server GUI. *For additional information, please refer to Note on Encryption at Rest on page 163.* • **Never:** (this is the default for new installations) Do not use EAR • **Optional:** User may choose at send time whether to encrypt or not • **Allow dropboxes to have their own encryption settings:** (off is the default for new installations) If this global setting is unchecked, you cannot set EAR for individual dropboxes. If checked, you can adjust EAR settings for each dropbox. Please see *Create and Manage Dropboxes* on page 124 for details.

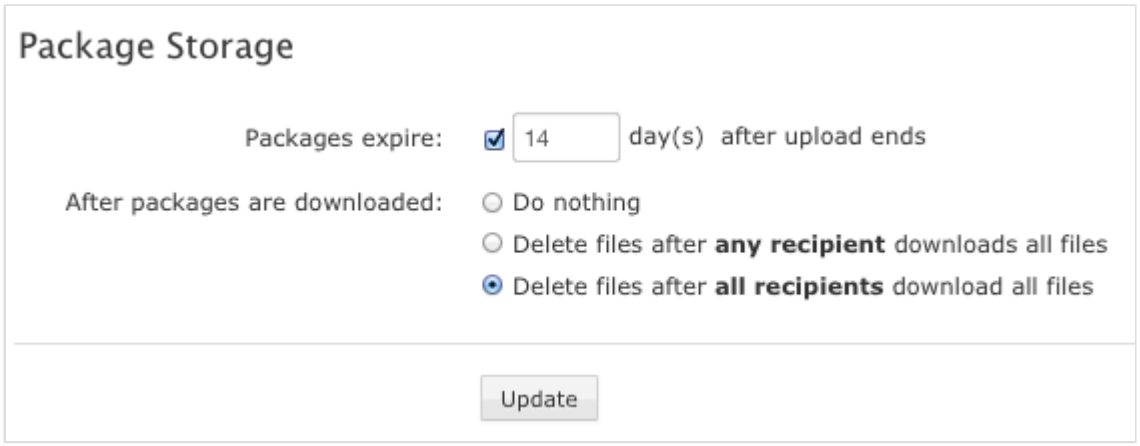
SAML

IMPORTANT NOTE: You must click the **Update** button to apply and save your changes.

Package Storage

Configure how your Faspex Server stores packages.

Within the Faspex Server Web UI, go to **Server** > **Configuration** > **Package Storage** to view and/or modify your server's package expiration and deletion behavior. After modifying these settings, you must click the **Update** button to save your changes.



Configuration Option	Description
Packages expire	Once a package is uploaded to the Faspex Server, the link to view the package will expire after the specified number of days.
After packages are downloaded	Select from one of the following auto-deletion rules: • **Do nothing:** Do not auto-delete after the package is downloaded. • **Delete files after any recipient downloads all files:** Delete after ANY recipient downloads ALL files in the package once. **IMPORTANT NOTE:** When this option is selected, a forwarded package can be potentially deleted before the original recipient has downloaded it. Thus, proceed with caution when selecting this option. • **Delete files after all recipients download all files:** Delete if ALL files in the package have been downloaded by ALL recipients.

IMPORTANT NOTE: The package storage location is your local docroot + the directory specified under your *Transfer Server* settings. The source location is the remote node's docroot + the file share location.

Display Settings

Configure your Faspex Server's display settings.

Within the Faspex Server Web UI, go to **Server** > **Configuration** > **Display Settings** to view and/or modify your server's date display format. The following list displays the variables that can be utilized, along with display samples:

Variable	Description and Sample
%a	The abbreviated weekday name (e.g., *Sun*).
%A	The weekday name (e.g., *Sunday*).
%b	The abbreviated month name (e.g., *Jan*).
%B	The month name (e.g., *January*).
%d	Day of the month (e.g., *01~31*).
%j	Day of the year (e.g., *001~366*).
%m	Month of the year (e.g., *01~12*).
%y	The abbreviated year (e.g., *09*).
%Y	The year (e.g., *2009*).

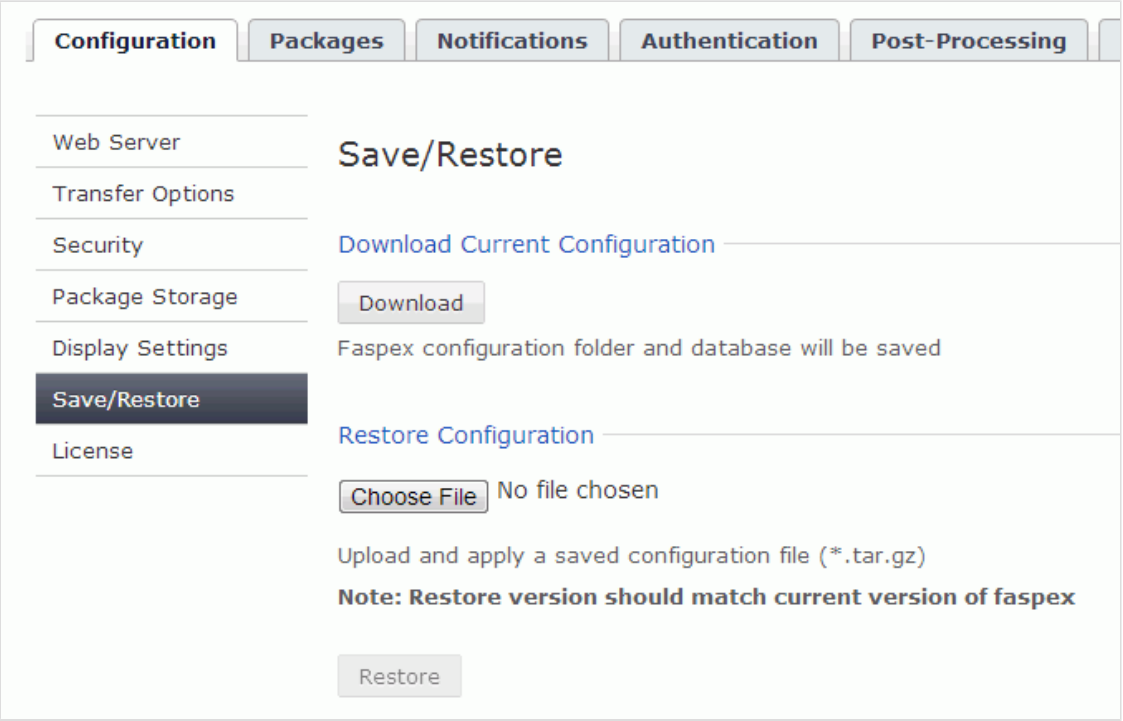
IMPORTANT NOTE: You must click the **update** button to apply and save your changes.

Save/Restore

Save and restore your Faspex configuration and database via the Web UI.

Within the Faspex Server Web UI, go to **Server** > **Configuration** > **Save/Restore** to save your current Faspex Server configuration and database.

IMPORTANT NOTE: *Aspera strongly recommends backing up your configuration and database in the event of a system failure*. The save/restore feature DOES NOT back up your Faspex packages, SSL Cert, and the transfer user's docroot to S3 storage, and it will not preserve the mapping between users and their packages. If you want to preserve these items, you need to back them up manually.



Click the **Download** button to save your current Faspex configuration folder and database in the format `*.tar.gz`. Conversely, you can restore your Faspex configuration folder and database by browsing for the corresponding `*.tar.gz` file on your system and clicking the **Restore** button. There are additional steps that you need to follow when restoring Faspex on a new machine. Please refer to the topic "*Restoring Faspex*" for details.

WARNING! Use caution when restoring your Faspex configuration and database! The restore version (that which you saved) *MUST* match your currently installed version of Faspex.

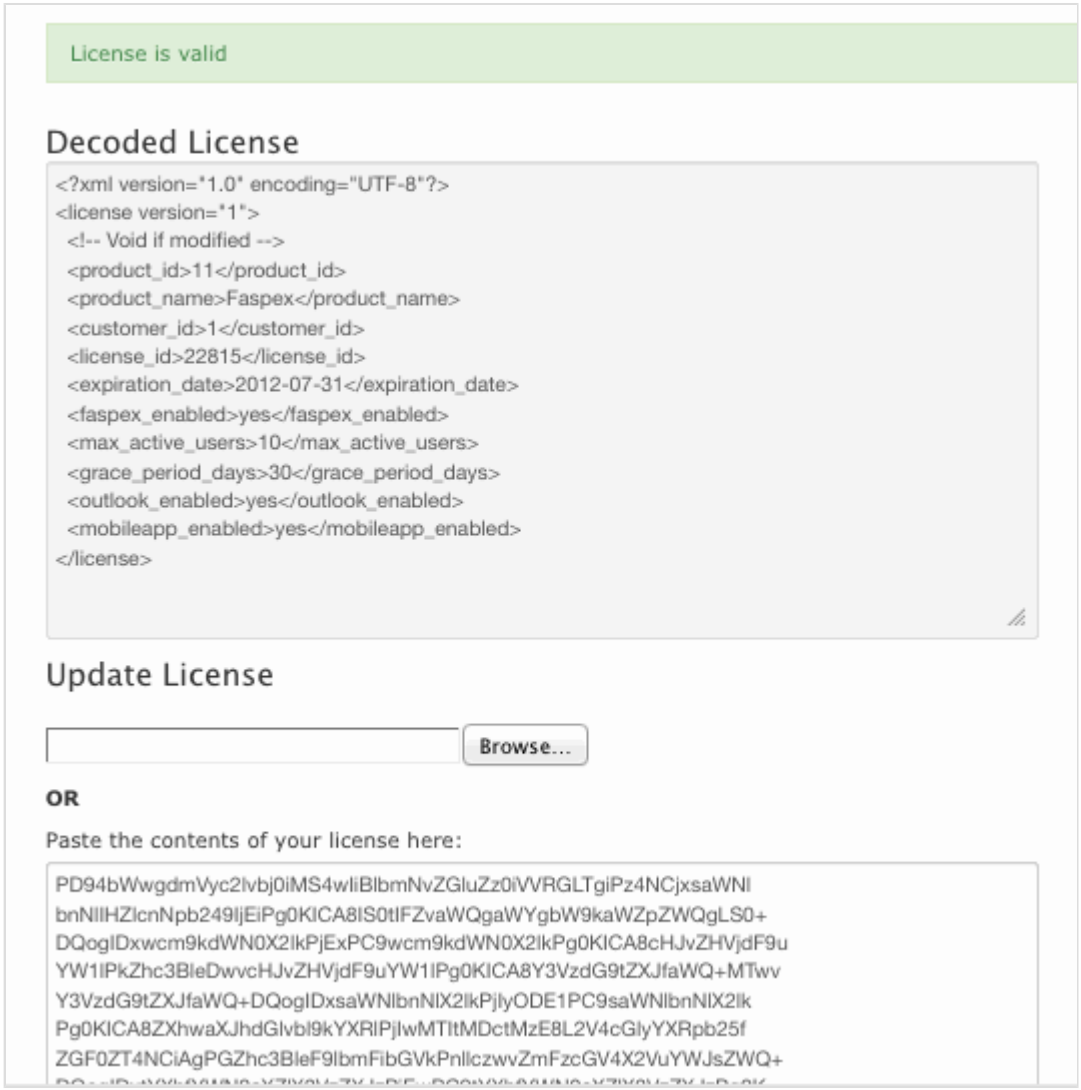
IMPORTANT NOTE: If you created *post-processing scripts*, you must copy and restore them manually. Faspex does not automatically save them for you. Additionally, if you have a custom SSL Certificate, or want to preserve the existing one, copy the SSL certificate(s) and key(s) to the following location and create a separate backup of the directory:

OS Version	File Location
32-bit Windows	C:\Program Files\Common Files\Aspera\Common\apache\conf\
64-bit Windows	C:\Program Files (x86)\Common Files\Aspera\Common\apache\conf\

License

Activate Faspex Server with your license key.

As Faspex Administrator, you can log in without activating Faspex Server; however, you must have a valid license key to configure your users and begin sending/receiving packages. As of Faspex Server v3.0+, you can install your license key using the Faspex Web UI. To import or paste your license key, log into your Faspex Server Web UI as Administrator, and go to **Server** > **Configuration** > **License** .



You will find your Faspex Server license key file (e.g., `aspera.faspex.*.aspera-license`) in an authorization email sent to you by Aspera. If you have not received this email or need it resent, please contact *Technical Support* on page 175 for assistance.

After you have pasted or imported your license, click the **Update and validate license** button.

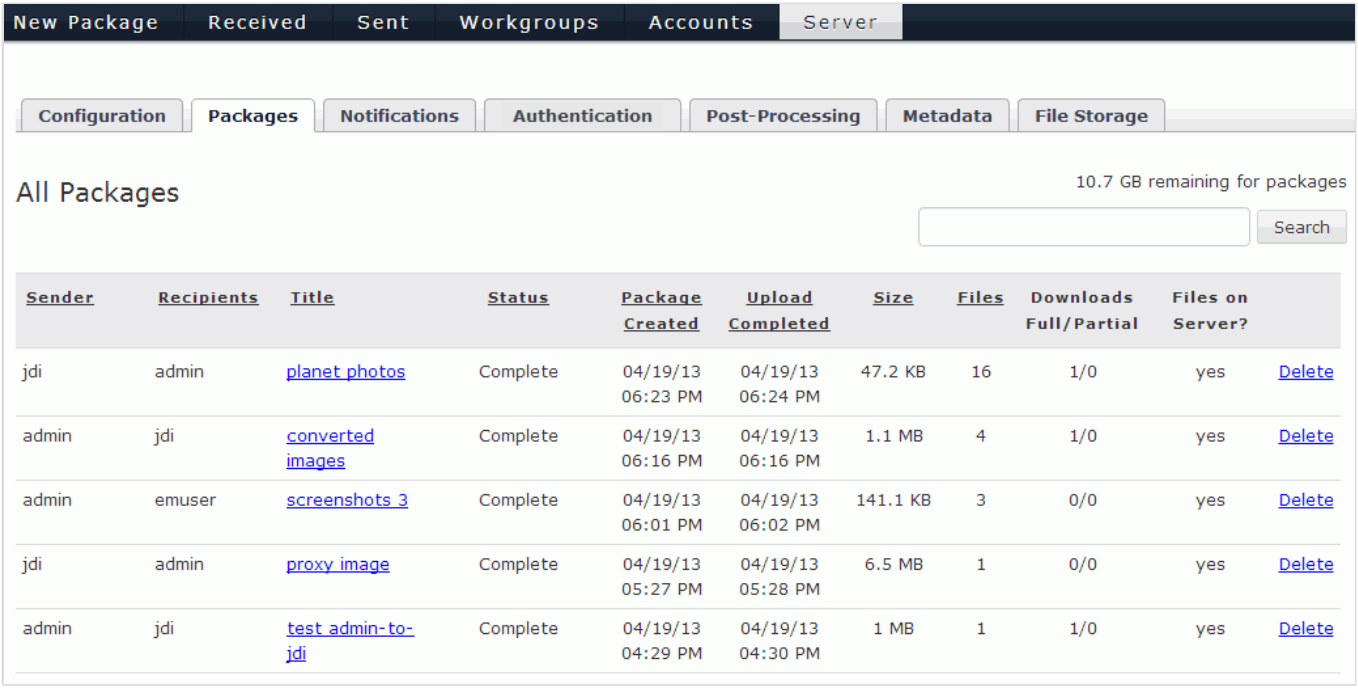
Additional Faspex Configuration Options

Additional configuration options for Faspex Administrators.

Packages

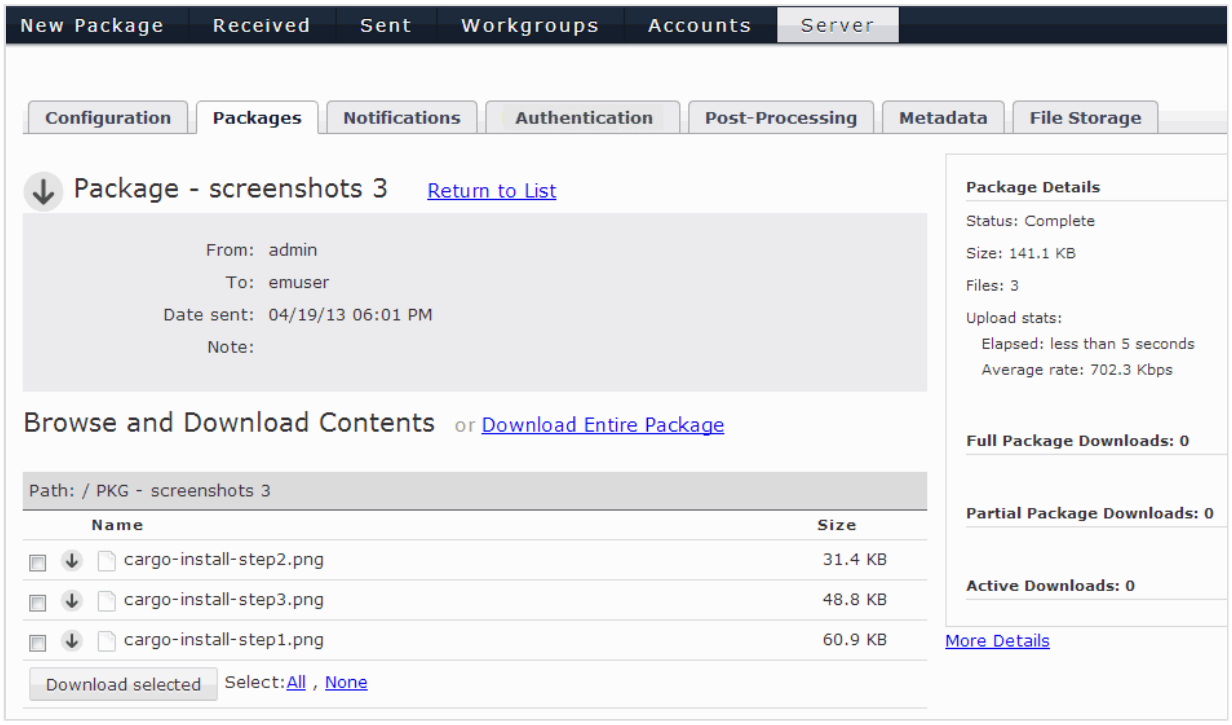
Manage file packages on Faspex Server

To view a list of packages sent via Faspex, as well as details like status, creation date/time, size, etc., go to **Server** > **Packages** .



Sender	Recipients	Title	Status	Package Created	Upload Completed	Size	Files	Downloads Full/Partial	Files on Server?	
jdi	admin	planet photos	Complete	04/19/13 06:23 PM	04/19/13 06:24 PM	47.2 KB	16	1/0	yes	Delete
admin	jdi	converted images	Complete	04/19/13 06:16 PM	04/19/13 06:16 PM	1.1 MB	4	1/0	yes	Delete
admin	emuser	screenshots 3	Complete	04/19/13 06:01 PM	04/19/13 06:02 PM	141.1 KB	3	0/0	yes	Delete
jdi	admin	proxy image	Complete	04/19/13 05:27 PM	04/19/13 05:28 PM	6.5 MB	1	0/0	yes	Delete
admin	jdi	test admin-to-jdi	Complete	04/19/13 04:29 PM	04/19/13 04:30 PM	1 MB	1	1/0	yes	Delete

Here, you will find the Faspex package list. To view the contents of any non-deleted package, simply click its hyperlinked title.



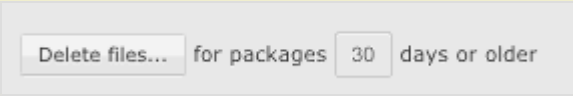
You may also sort the package list by one of the following column headers:

- Sender name
- Recipient(s) name
- Title
- Status (i.e. completed or stopped)
- Package Created (date and time)
- Upload Completed (data and time)
- Size
- Number of Files (included in package)

Click a column header to sort the list. Click a second time to reverse the sort order. Note that three additional columns exist:

- **Downloads Full/Partial:** The number of times the corresponding package has been fully or partially downloaded.
- **Files on Server?:** (Yes, Deleted or Partial) States whether or not the package is currently stored on the server. "Yes" indicates that all files in the package have been uploaded; "Partial" indicates that some of the files in the package have been uploaded; and "Deleted" indicates that the package and its files have been deleted from the server.
- **Delete:** If you see an active Delete hyperlink, then you may click it to delete the corresponding package from the server. If the package has already been deleted from the server, then the entire row will be grayed out and the field **Files on Server** will display "No."

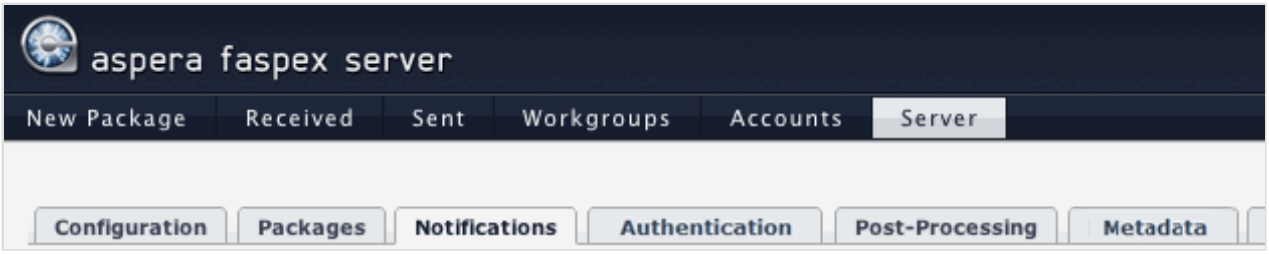
IMPORTANT NOTE: You can also perform a batch deletion for packages that are older than "X" number of days. To do so, scroll to the bottom of the packages list and enter the number of days in the **for packages [x] days or older** field. "X" is set to 30 days, by default; however, you can input another value at your discretion. Click the **Delete files...** button to proceed with the deletion.



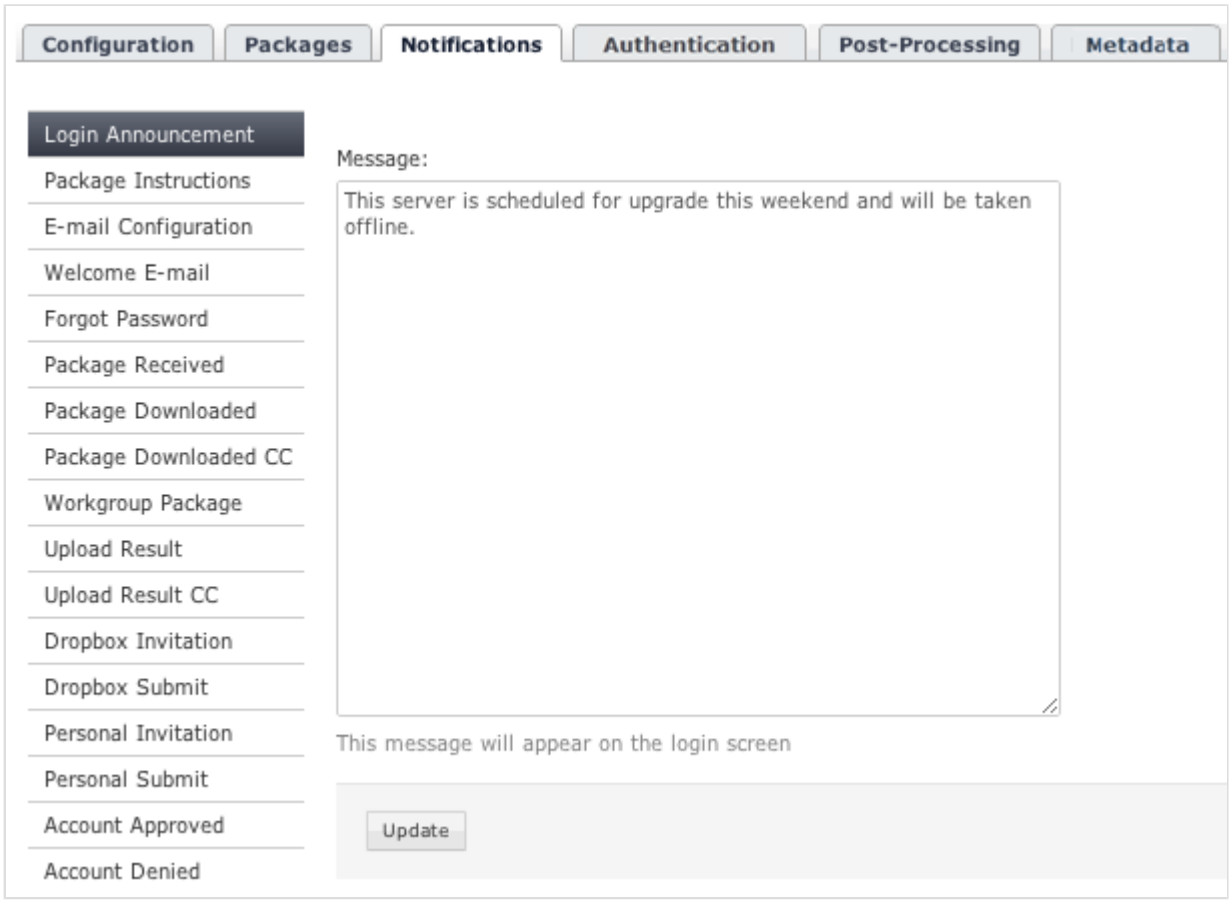
Notifications

Configure Faspex notifications for various events.

As a Faspex Server Administrator, you can communicate with your users regarding various events using the Faspex "Notifications" feature. This topic describes the types of notifications available within Faspex. To get started, go to **Server** > **Notifications** within the Faspex Web UI.

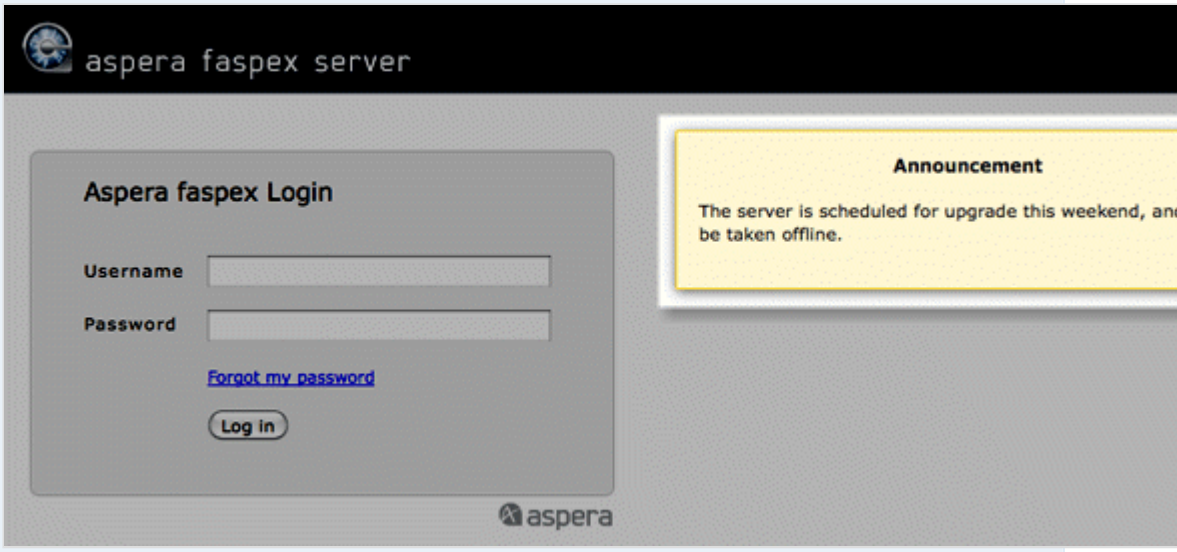
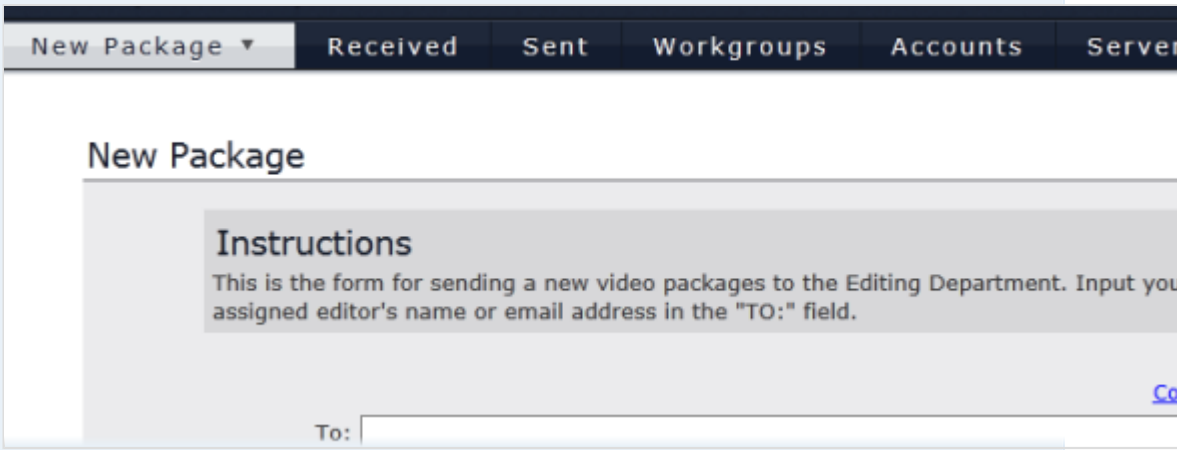


The following notification options appear on the left-side of the screen:



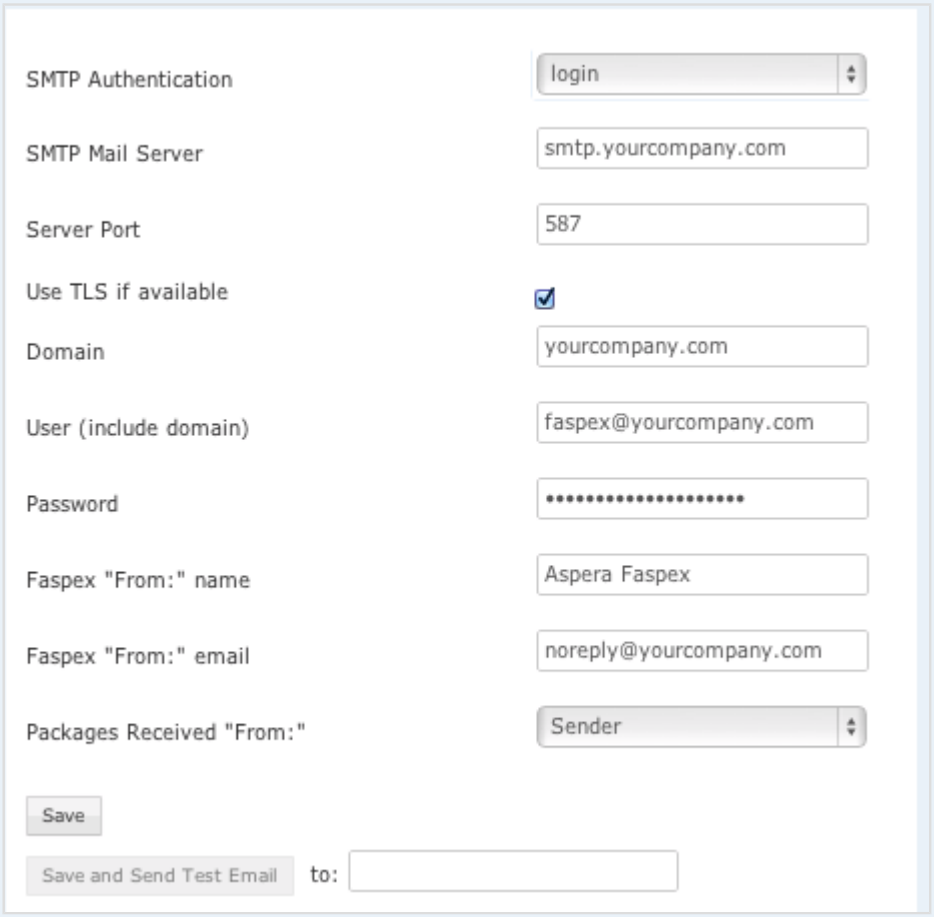
IMPORTANT NOTE: Notification types 4 through 17, below, utilize the same editing interface and only vary in content. When you select one of these notification types, you can edit its respective content by clicking the **Customize Using Template** or **Edit HTML** links. The **Customize Using Template** option enables you to create an email template using a form (which includes the ability to insert text strings), while the **Edit HTML** allows you to create an email template with HTML code. Do not use HTML or the < and > symbols when editing content via **Customize Using Template**! You will find a list of each notification type's available text strings below this table.

#	Notification Type	Description
1	Login Announcement	Post an announcement for users on your organization's Faspex login page. Once saved, your announcement message will appear on the login page, as shown below.

#	Notification Type	Description
		
2	Package Instructions	Post instructions for users who are sending new, normal packages (i.e., NOT dropbox packages). Once saved, your instructions will appear on the Faspex normal "New Package" screen (example is shown below).  **IMPORTANT NOTE:** *Dropbox package* instructions can be created and/or edited from the **Workgroups** > **(Down Arrow)** > **Edit Dropbox** menu (see the Instructions for submitters field in the topic *Create and Manage Dropboxes* on page 124).
3	E-mail Configuration	Input your email (SMTP) server settings for sending notifications from Faspex. Settings include the following: • SMTP Authentication: Open or login • SMTP Mail Server

#	Notification Type	Description
		• Server Port • Use TLS if available: Enable or disable. Please refer to the **IMPORTANT NOTE** below. • Domain • User: The email account that you are sending the notification from (be sure to include the domain). • Password: The email account's password. • Faspex "From" name: The "from" name that appears on Faspex-generated emails. • Faspex "From" email: The "from" email address that appears on Faspex-generated emails. • Packages received "From": Choose from Sender, Faspex, Sender via Faspex. If *Sender* is selected, package notifications will show as being received from "Sender's Name." If *Faspex* is selected, package notifications will show as being received from "Faspex." If *Sender via Faspex* is selected, package notifications will show as being received as the "Sender's Name via Faspex." **IMPORTANT NOTE ON TLS:** Faspex will confirm whether or not the name in your TLS security certificate matches your mail server's configured address (fully qualified domain name and/or IP address). If it does not, you will receive an error. If your fully qualified domain name does not resolve with your internal DNS, you must add the IP address and name to your `/etc/hosts` file (or ensure the name resolves using DNS).

#	Notification Type	Description



IMPORTANT NOTE: If your Faspex Server is configured to identify itself by IP address (rather than by domain name), then the URLs in your notification emails will contain an IP address (e.g. "https://10.0.0.1/aspera/faspex"). Some Web-based email services (e.g. Yahoo or Ymail, Hotmail, etc.) have been known to automatically flag emails containing IP address links as "Spam," and will move them to your Junk/Spam folder. For this reason, Aspera recommends creating a domain name for your Faspex Server. If you do not have a domain name immediately available, then you can initially configure Faspex with an IP address and then change it to use a domain name later. If you know that you will not be setting up a domain name, then make sure that users add your Faspex "From" email address (e.g. faspex_admin@yourcompany.com) to their address book and/or contact list. Doing so typically "white-lists" the address so that emails from your Faspex Server are not automatically flagged and routed to your users' Junk/Spam boxes.

To debug your SMTP server settings, enter your email address in the **Save and Send Test Email** text field, and click the button to send a test email.

#	Notification Type	Description
4	Welcome E-mail	Informs a user that his or her account is ready for use, and includes steps to get started. *Jump to text strings*.
5	Forgot Password	Allows a user to reset his or her password. A user can request to have this email sent from the login screen. *Jump to text strings*.
6	Package Received	Informs users when they receive packages. *Jump to text strings*.
7	Package Downloaded	Informs users when a sent package has been downloaded. For details, see *Note on Download Notifications* below. *Jump to text strings*.
8	Package Downloaded CC	Informs anyone CC'd on a package download when someone downloads the package. For details, see *Note on Download Notifications* below. *Jump to text strings*.
9	Workgroup Package	Informs users when packages are sent to workgroups they belong to. *Jump to text strings*.
10	Upload Result	Sent to a package sender or dropbox submitter when the upload ends, providing information on whether it completed successfully or not. *Jump to text strings*.
11	Upload Result CC	Sent to anyone CC'd on a package upload, providing information on whether it completed successfully or not. *Jump to text strings*.
12	Dropbox Invitation	Sent to outside users when invited to submit to a dropbox. *Jump to text strings*.
13	Dropbox Submit	Sent when an outside user submits a package to a dropbox. *Jump to text strings*.
14	Personal Invitation	Sent to outside users after submitting their email address via the public URL feature. This invitation contains a private link for package submission. *Jump to text strings*.
15	Personal Submit	Sent to outside users after they have submitted a package via a user's or workgroup's public URL. It also provides them with information for checking their package status. *Jump to text strings*.
16	Account Approved	Prompts new, self-registered users to activate their accounts by resetting the password. *Jump to text strings*.
17	Account Denied	Sent to an account requester when the requested account has been denied by an Administrator. *Jump to text strings*.

NOTE on DOWNLOAD NOTIFICATIONS:

- If a sender of a package downloads the sent package, no users are notified.
- If a recipient downloads a package and is included on the CC list, he receives a download notification.
- If an admin downloads a package from the **Server > Packages** page, all download CC recipients are notified, even if the admin is not the sender or recipient of the package.
- If a private recipient downloads a package, all download CC recipients are notified, and the private recipient's name is thereby revealed.

- If a package is only partially downloaded, all download CC recipients are notified; however, the notification does not indicate that the download was partial.

Welcome E-mail

Variable	Description
USER_NAME	Email recipient's full name
LOGIN	Email recipient's login (user account) name.
SERVER_ADDRESS	Faspex Server name or IP address

Forgot Password

Variable	Description
USER_NAME	Email recipient's full name
LOGIN	Email recipient's login (user account) name.

Package Received

Variable	Description
SENDER_NAME	Sender's full name
SENDER_EMAIL	Sender's email address
SENDER_LOGIN	Sender's login (user account) name
USER_NAME	Email recipient's full name
PACKAGE_NAME	Package name
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the packag.
PACKAGE_NOTE	Message associated with the package

Package Downloaded and Package Downloaded CC

Variable	Description
DOWNLOADER_EMAIL	Downloader's email address

Variable	Description
DOWNLOADER_NAME	Downloader's full name
DOWNLOADER_LOGIN	Downloader's login (account user) name
SENDER_NAME	Sender's full name
PACKAGE_NAME	Package name
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_NOTE	Message associated with the package

Workgroup Package

Variable	Description
USER_NAME	Recipient's full name
WORKGROUP_NAME	Name of the workgroup that the package was sent to
SENDER_NAME	Sender's full name
SENDER_EMAIL	Sender's email address
SENDER_LOGIN	Sender's login (user account) name
PACKAGE_NAME	Package name
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_NOTE	Message associated with the package

Upload Result and Upload Result CC

Variable	Description
SENDER_EMAIL	Sender's email address
PACKAGE_NAME	Package name
PACKAGE_DATE	Package's sent date

Variable	Description
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_NOTE	Message associated with the package
UPLOAD_RESULT	The result of the dropbox submission upload
STATUS_URL	URL to check package upload status
STATUS_LINK	Link to check package upload status

Dropbox Invitation

Variable	Description
EMAIL	Email address of the invited outside email user
DROPBOX_NAME	Dropbox to which the outside email user was invited
DROPBOX_URL	The URL that the outside email user can use to send packages to the dropbox
DROPBOX_LINK	HTML link that the outside email user can use to send packages to the dropbox

Dropbox Submit

Variable	Description
DROPBOX_NAME	Dropbox to which the outside email user was invited
PACKAGE_NAME	Package name
PACKAGE_DATE	Package's sent date
PACKAGE_NOTE	Message associated with the package
STATUS_URL	URL to check package upload status

Personal Invitation

Variable	Description
EMAIL	Email address of the invited outside email user
RECIPIENT_NAME	Recipient who invited the outside email
SUBMISSION_URL	The URL that the outside email user can use to send a package

Variable	Description
SUBMISSION_LINK	HTML link that the outside email user can use to send a package
LINK_EXPIRATION_INFO	If the submission link expires, a sentence describing when the link expires

Personal Submit

Variable	Description
RECIPIENT_NAME	Name of the recipient of the sent package
SENDER_EMAIL	Email address of the sender
PACKAGE_NAME	Package name (for which relay failed)
PACKAGE_NAME	Package name
PACKAGE_DATE	Package's sent date
PACKAGE_NOTE	Message associated with the package
STATUS_URL	URL to check package upload status
STATUS_LINK	Link to check package upload status

Account Approved and Account Denied

Variable	Description
USER_NAME	Full name of the e-mail recipient
SERVER_ADDRESS	Name or IP of the Faspex server
LOGIN	Login name of the e-mail recipient

Authentication: Directory Service

Import your organization's directory service users and groups into Faspex.

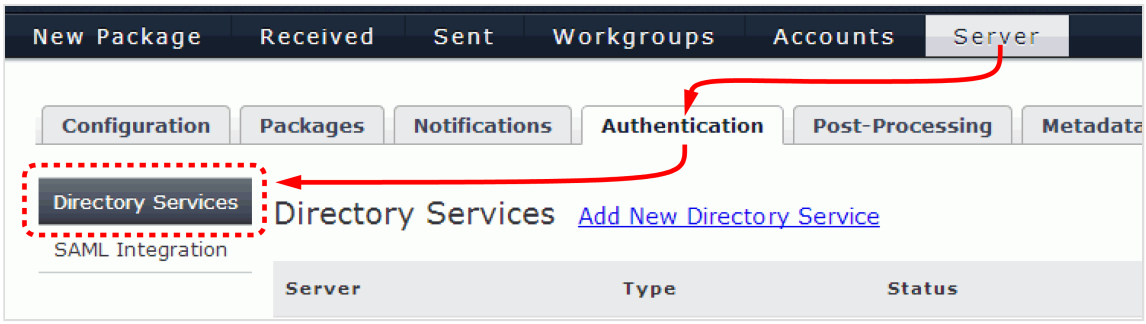
Faspex supports the Lightweight Directory Access Protocol (LDAP) and can be configured to connect to a directory service. The following directory service databases are supported:

- 389/Red Hat/Fedora Directory Server
- Apple Open Directory
- Microsoft Active Directory (AD)

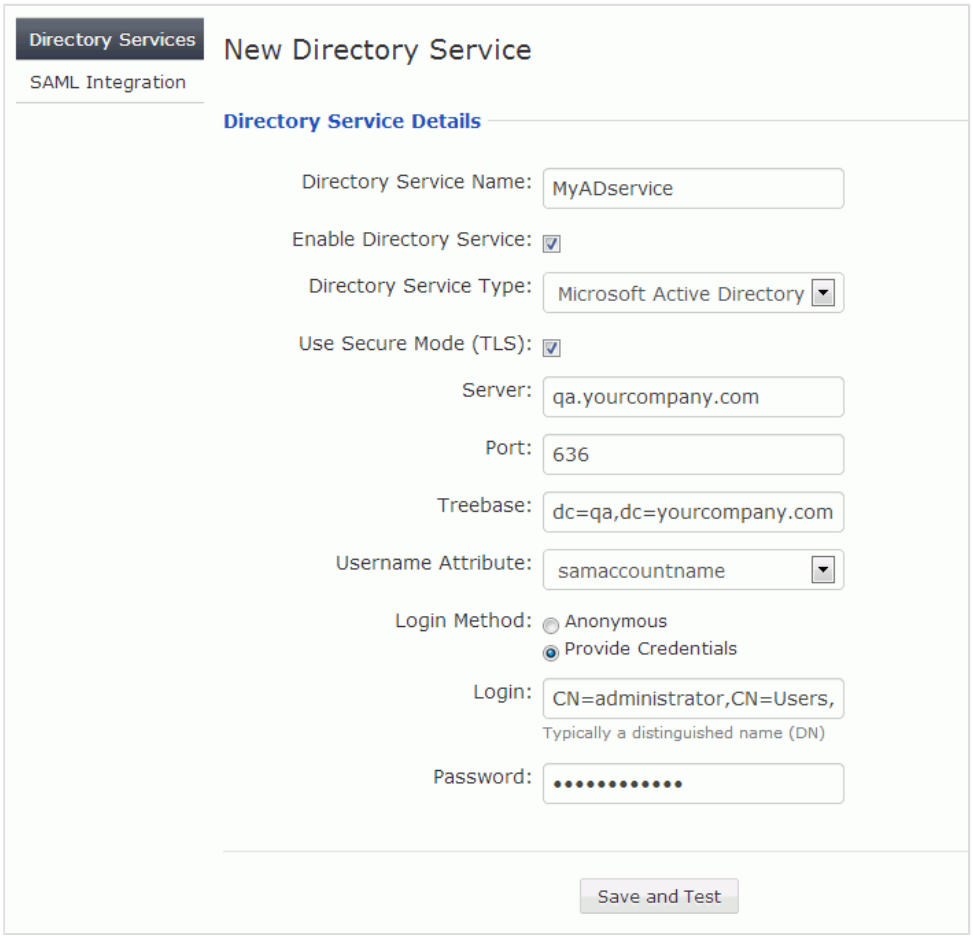
Follow the steps below to configure Faspex for LDAP.

1. Enter directory service details

   Go to **Server** > **Authentication** > **Directory Services** .



   To configure your directory service to work with Faspex, check **Enable Directory Service** and enter your configuration details (example displayed below).



Option	Description
Directory Service Name	Your name for this directory service.

Option	Description
Enable Directory Service	Activate this directory service for Faspex.
Directory Service Type	Select from one of the following options: • 389/Red Hat/Fedora Directory Server • Apple Open Directory • Microsoft Active Directory (AD)
Use secure mode (TLS)	***NOTE: Aspera highly recommends turning this setting on to secure your server.*** By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by enabling TLS. The port number will automatically change to 636 when TLS is enabled.
Server	The directory server's address.
Port	The directory server's port number. By default, unsecured LDAP uses port 389, unsecured global catalog uses port 3268, and global catalog over SSL uses port 3269. If TLS is enabled, then the port number will automatically change to 636.
Treebase	The search treebase *(e.g. dc=myCompany,dc=com for myCompany.com)*
Username Attribute	The attribute for the type of logon name for users of this directory service. For example, for Microsoft Active Directory, the **mail** attribute specifies the DS user logon should be an email address, and **samaccountname** specifies it should be a pre-Windows 2000 logon name.
Login Method	• Anonymous • Provide Credentials If *Provide Credentials* is selected, then you are required to input your directory service login and password below.
Login	Directory service user name, which is typically a Distinguished Name (DN) (e.g. CN=Administrator,CN=Users,DC=myCompany,DC=com).
Password	Directory service password.

When finished, click **Save and Test**. If Faspex successfully connects to your directory server, it displays the following information:

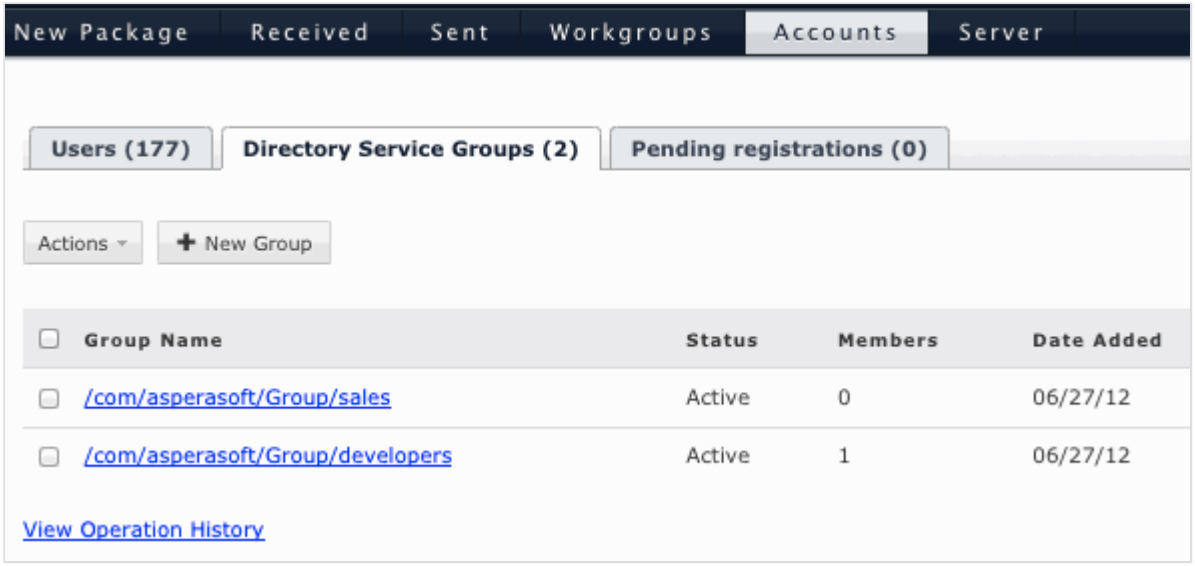
```
Connected: YES
Authenticated: YES
Success
```

NOTE: If the same user (identified by the username attribute) is a member of more than one directory, the user is only imported once from the first sync. The duplicated user from the second directory is not imported, and a warning is logged in the sync history.

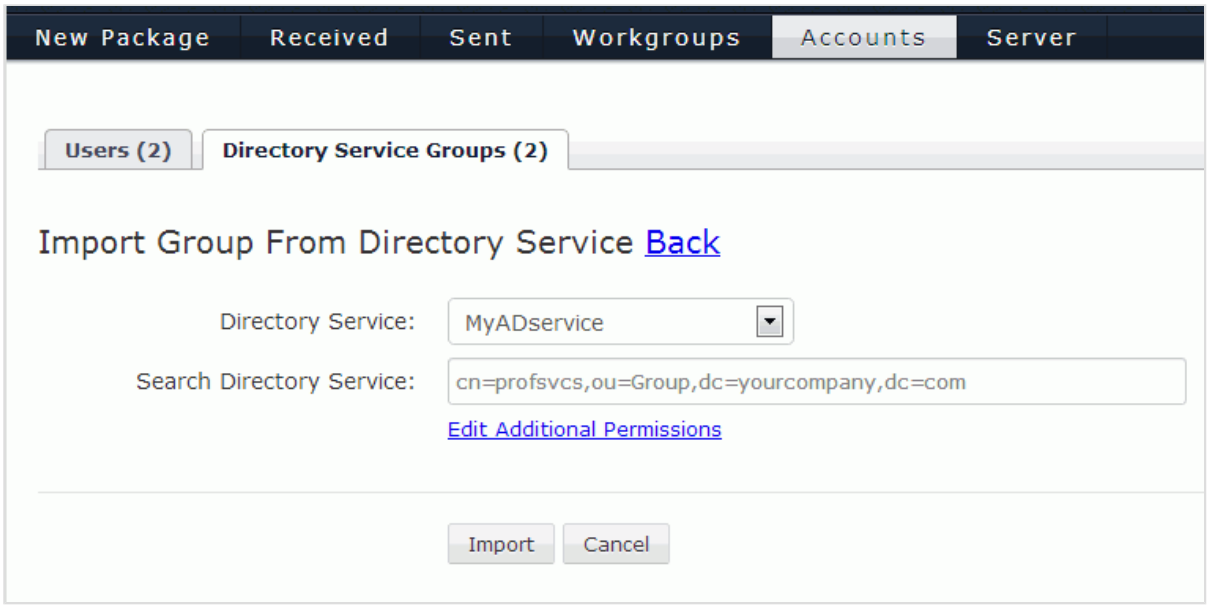
2. Import Directory Service (DS) groups

IMPORTANT NOTE: When Faspex Server imports AD groups, it is bounded by the AD server parameter "MaxValRange." If you would like to import a larger AD group, then please change the "MaxValRange" parameter on your AD server.

When importing a Directory Service group, all users listed under that group are added into Faspex. To import a group, start by going to **Accounts** and select the **Directory Service Group** tab. Any DS groups that you have previously imported are shown in the list.

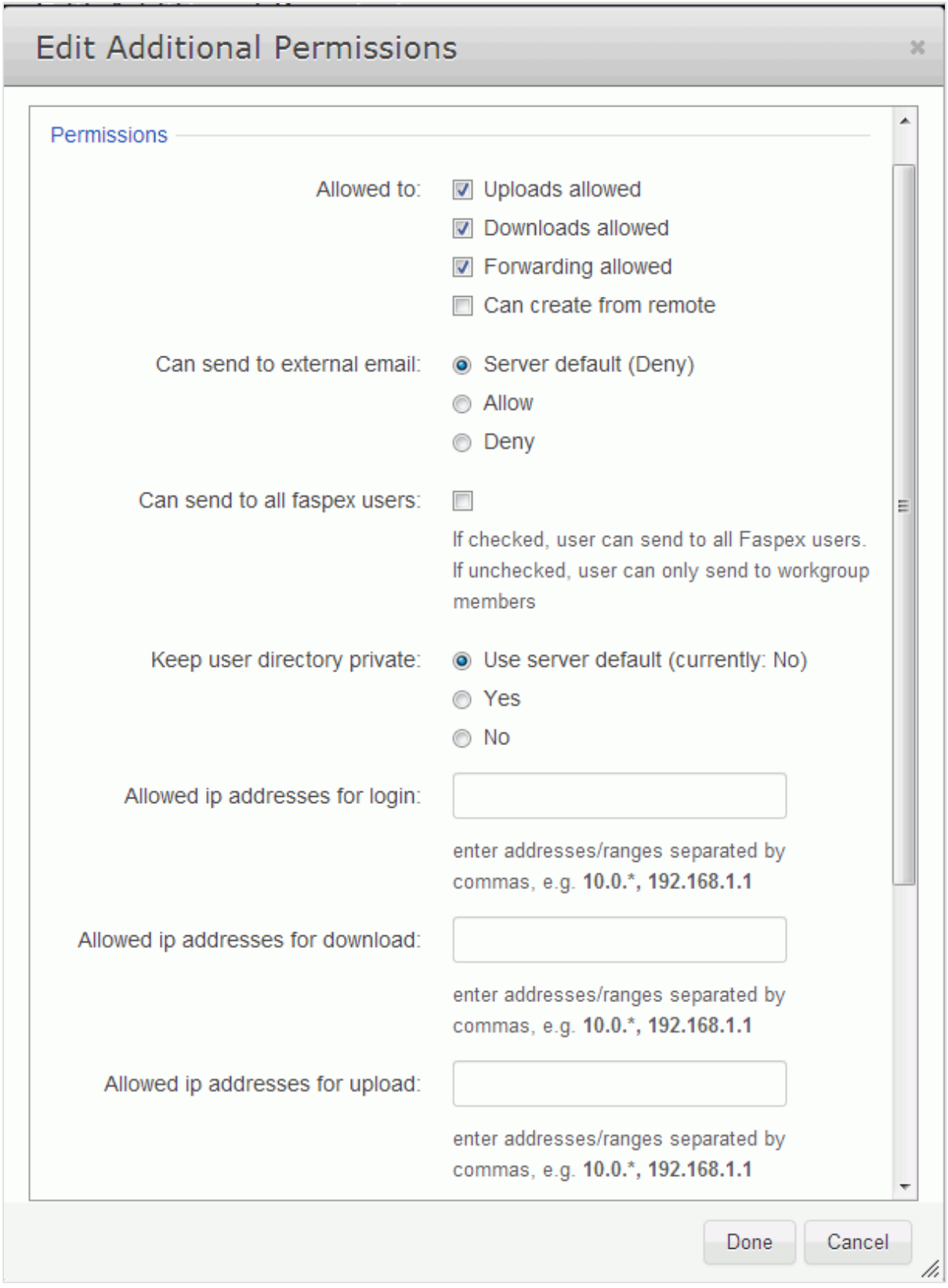


From here, click the **+ New Group** button and enter the directory service group attributes. Typing three characters or more brings up the group list with matching keywords.



IMPORTANT NOTE: You cannot import Directory Service groups that have the same name, regardless of whether or not they are on the same DS server. All DS groups must have unique names.

To specify permissions for this DS group, click the **Edit Additional Permissions** link. The Edit Additional Permissions dialog appears:

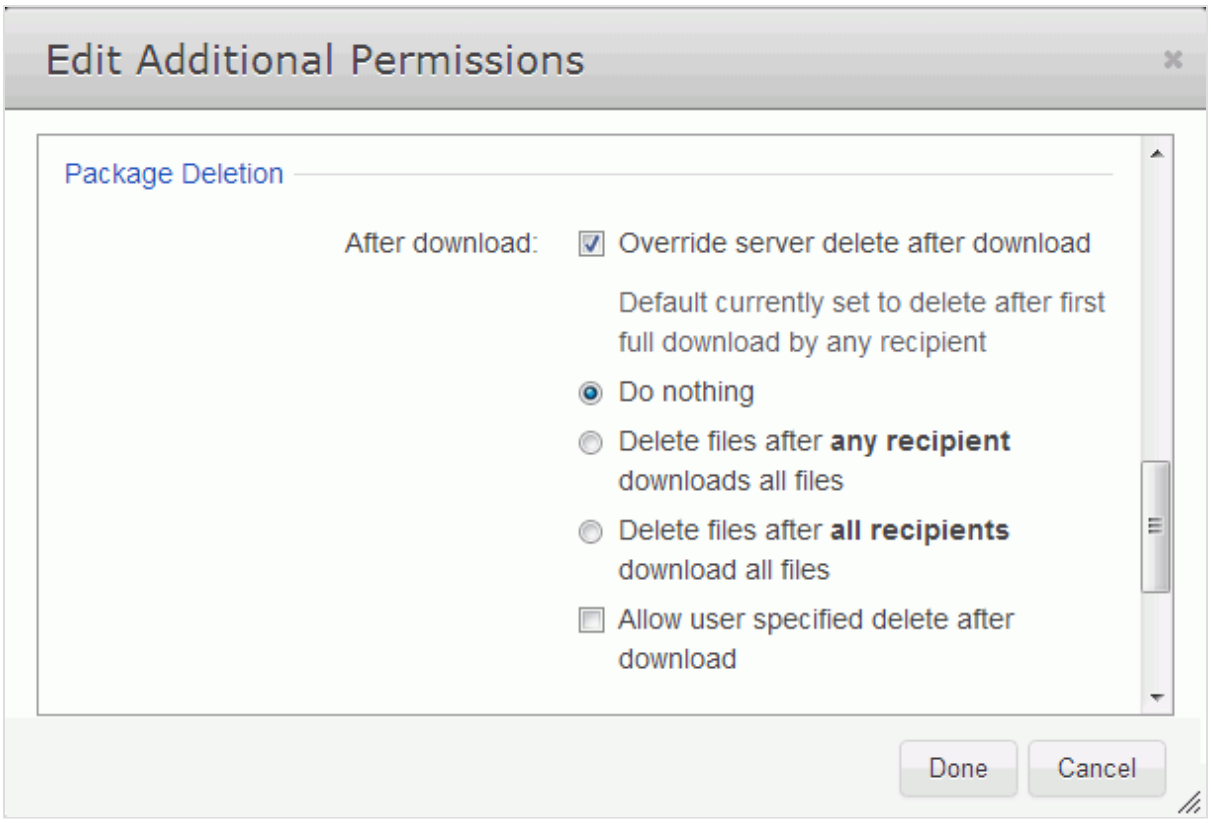


Permissions

Option	Description
Uploads allowed	Enable to allow the user to send file packages.
Downloads allowed	Enable to allow the user to download packages that have been received. A user who does not have this marked will still receive packages, but will not be able to download the files.
Forwarding allowed	Enable to allow the user to forward received file packages to other users. The package will be made accessible to the forwarded users within their Faspex accounts.
Can create from remote	Enable to allow the user to send packages from remote file storage.
Can send to external email	Allow or deny the user to send download links to external emails addresses (which are not Faspex users).
Can send to all Faspex users	Enable to allow the user to send packages to all Faspex users (as opposed to only being able to send to the user's workgroup members).
Allowed IP addresses for login	Specify the IP address(es) that a Faspex user can log in from to view his or her account. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).
Allowed IP addresses for download	Specify the IP address(es) that a Faspex user can login from to download packages. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).
Allowed IP addresses for upload	Specify the IP address(es) that a Faspex user can login from to upload packages. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).

Package Deletion

Scroll down the Edit Additional Permissions dialog to Package Deletion for options available **after downloading** a package:



Option	Description
Override server delete after download	The Faspex Server's current default auto-deletion settings are displayed just below this checkbox. Checking the box expands the dialog to let you override the default settings with one of the following policies: • Do nothing (i.e., do not delete files after downloads) • Delete files after **any recipient** downloads all files • Delete files after **all recipients** download all files To update the default setting, see *Package Storage* on page 62.
Allow user-specified delete after download	Follow the policy settings in the user's **New Package** screen. The user determines the file package's expiration rule when preparing it.

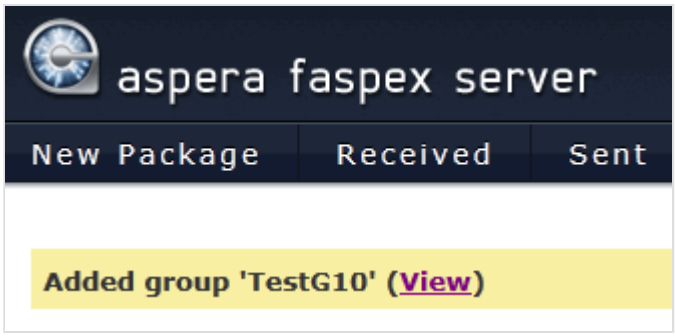
Advanced Transfer Settings

Faspex uses the transfer settings from the Aspera Central Server section by default. To override, scroll down the Edit Additional Permissions dialog to Advanced Transfer Settings. When **Override default settings** is checked, the dialog expands to allow you to set user-specific transfer settings, which will take precedence over the server-wide settings.

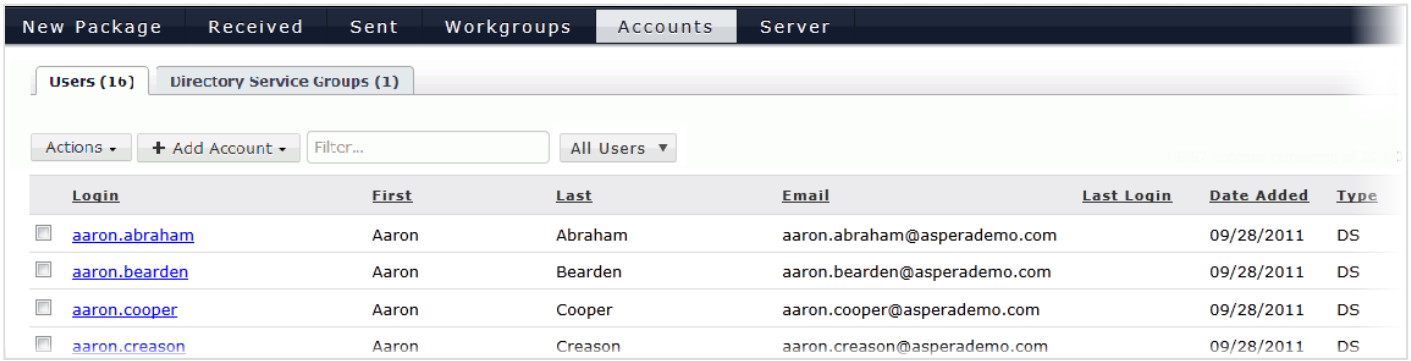
Option	Description
Initial Transfer Rate	Specify the initial upload and download transfer rate. When the option **Lock minimum rate and policy** is checked, the user will not be able to adjust transfer policy or minimum transfer rate.
Maximum Allowed Rate	Specify the initial upload and download transfer rate.

Click **Done** > **Import** when finished.

When adding directory service groups, Faspex searches for groups recursively to import users. For example, if group A contains Group 1, importing Group A also imports Group 1's members. Once imported, the directory service group's members are added to your Faspex Server and the import page is updated with a link to view/edit the new group.

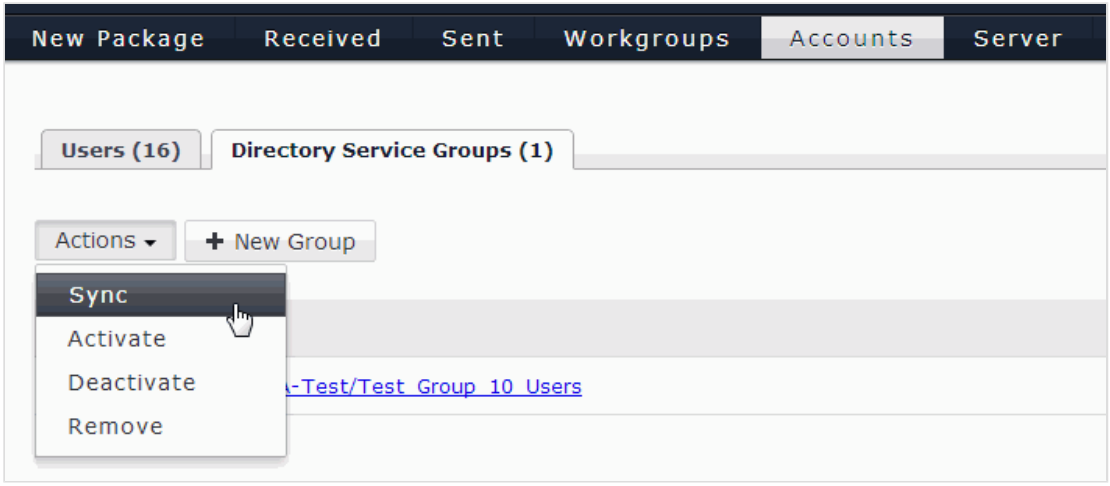


Click the **View** link to go back to the **Accounts** screen. Your imported DS users will appear in the accounts list, along with the type column identification *DS*.



Under the Directory Service Groups tab, you can administer a group by checkmarking the corresponding row and clicking on the **Actions** button. The **Actions** button contains the following functions:

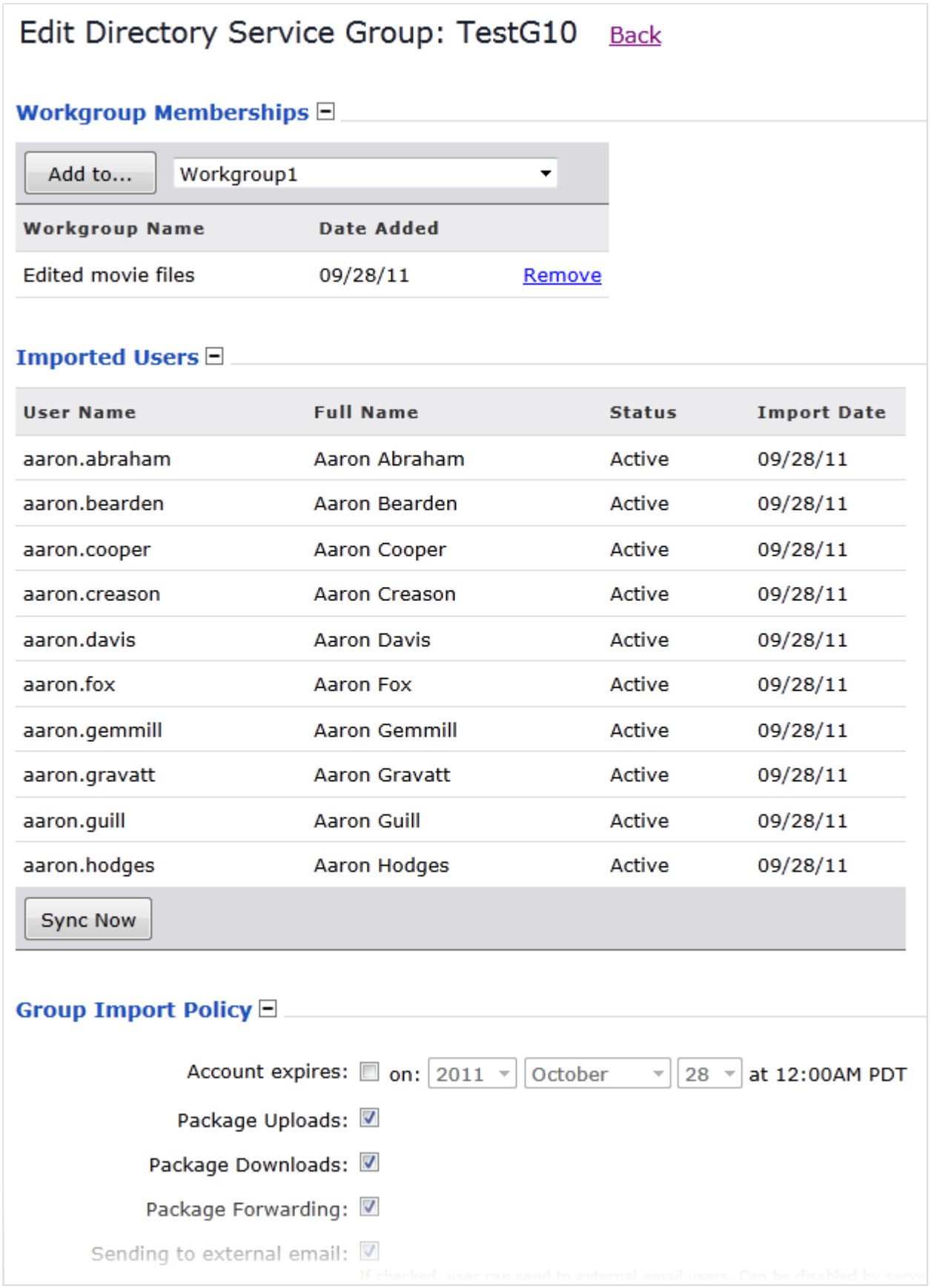
- Manually **Sync** with the directory server. Note that Faspex auto-syncs with the directory server every hour.)
- **Deactivate** and **Activate** disables or enables selected groups, respectively.
- **Remove** deletes the group.



IMPORTANT NOTES:

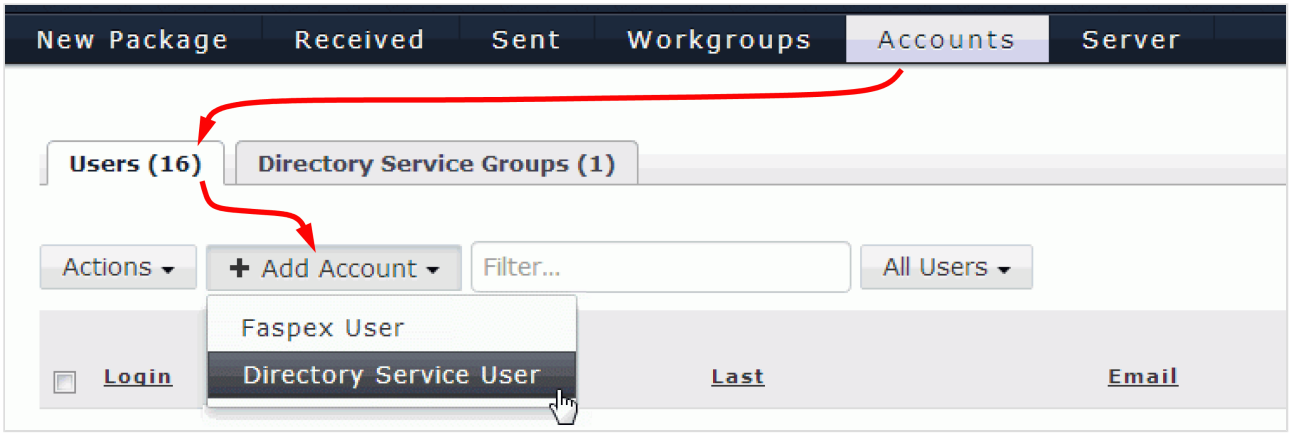
- Directory service syncing is accomplished through a Faspex background service that must be kept running.
- When removing a directory service group, users in that group are deactivated instead of removed.
- When a user exists in multiple directory service groups, removing one of the groups doesn't affect the user. The user is deactivated only when all the user's directory service groups are removed.
- An activated directory service group is shown as "Active" in the status column. If it shows otherwise, click **View Operation History** to read the Active Directory operation log and identify the problem.

To view the members of the DS group, update its workgroup memberships, or edit the DS users' Faspex settings and permissions, click the corresponding hyperlink to go to the *Edit Directory Service Group* screen.

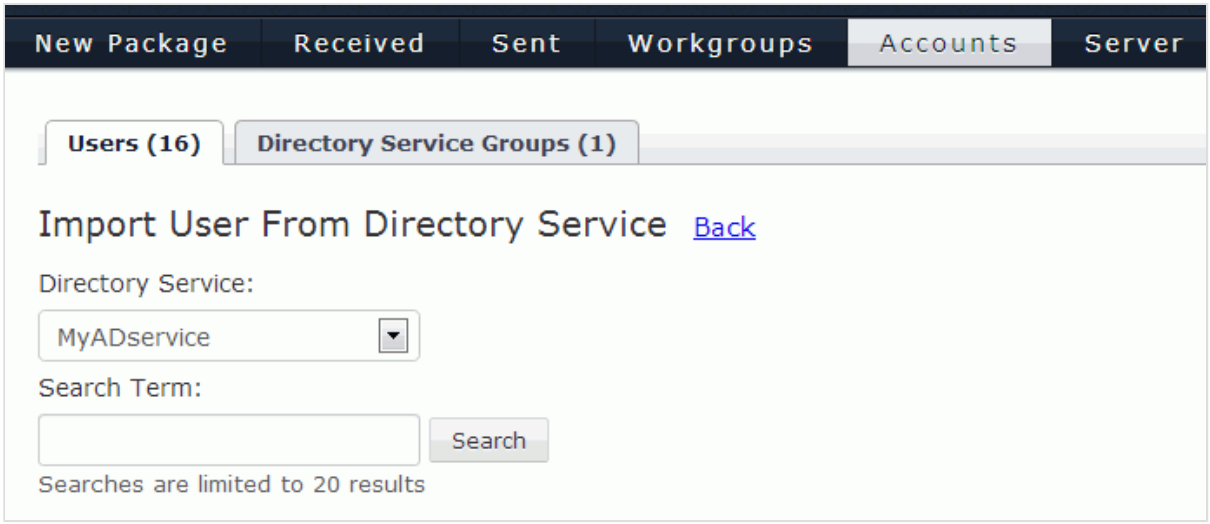


3. Import individual DS users (in addition to, or rather than, DS groups)

Start by going to **Accounts** > **Users** > **+Add Account** > **Directory Service User** .



The **Import User From Directory Service** page opens:



From the Directory Service dropdown box, first select the directory service that contains the users you want to import.

Then, in the Search Term box, enter a search string or substring for the user you want. A list of DS user accounts containing that string is displayed.

Select the name of the user to import. You can only import one user at a time.

Then, click **Edit Additional Permissions** at the bottom of the page.

In the page that appears, fill in the **Account Details** section, specifying whether this user is an admin, a manager, or a regular user. Then scroll down and fill in **Permissions**, **Package Deletion**, and other remaining sections, following the same procedure as described above for directory service groups (see Step 2 above).

IMPORTANT NOTE: Faspex syncs individual directory service users every hour. You cannot sync them manually.

Once directory service users (or groups) are imported, the corresponding users can authenticate with and log in to Faspex Server. Directory service accounts are similar to Faspex user accounts, although options such as changing the login password are deactivated (since this information is configured on the directory server).

Authentication: SAML

Integrate SAML authentication into Faspex.

Faspex supports Security Assertion Markup Language (SAML) 2.0, an open, XML-based standard that allows secure web domains to exchange user authentication and authorization data. With the SAML model, you can configure the Faspex web application as a SAML "online service provider" (SP) that contacts a separate online "identity provider" (IdP) to authenticate users who will use Faspex to access secure content.

With SAML enabled and configured, a user logging into Faspex is redirected to the IdP sign-on URL. If the user has already signed in with the IdP, the IdP sends a SAML assertion back to Faspex. The user is now logged into Faspex.

These instructions assume you are already familiar with SAML and already have an identity provider (IdP) -- either third-party or internal -- that meets the following requirements:

- can be configured to use an HTTP POST binding
- can be connected to the same directory service being used by Faspex
- will not be configured to use pseudonyms
- can be configured to return assertions to the SP (Faspex) that include the entire contents of the signing certificate

Enabling SAML Authentication in Faspex

Enable SAML authentication in Faspex as follows:

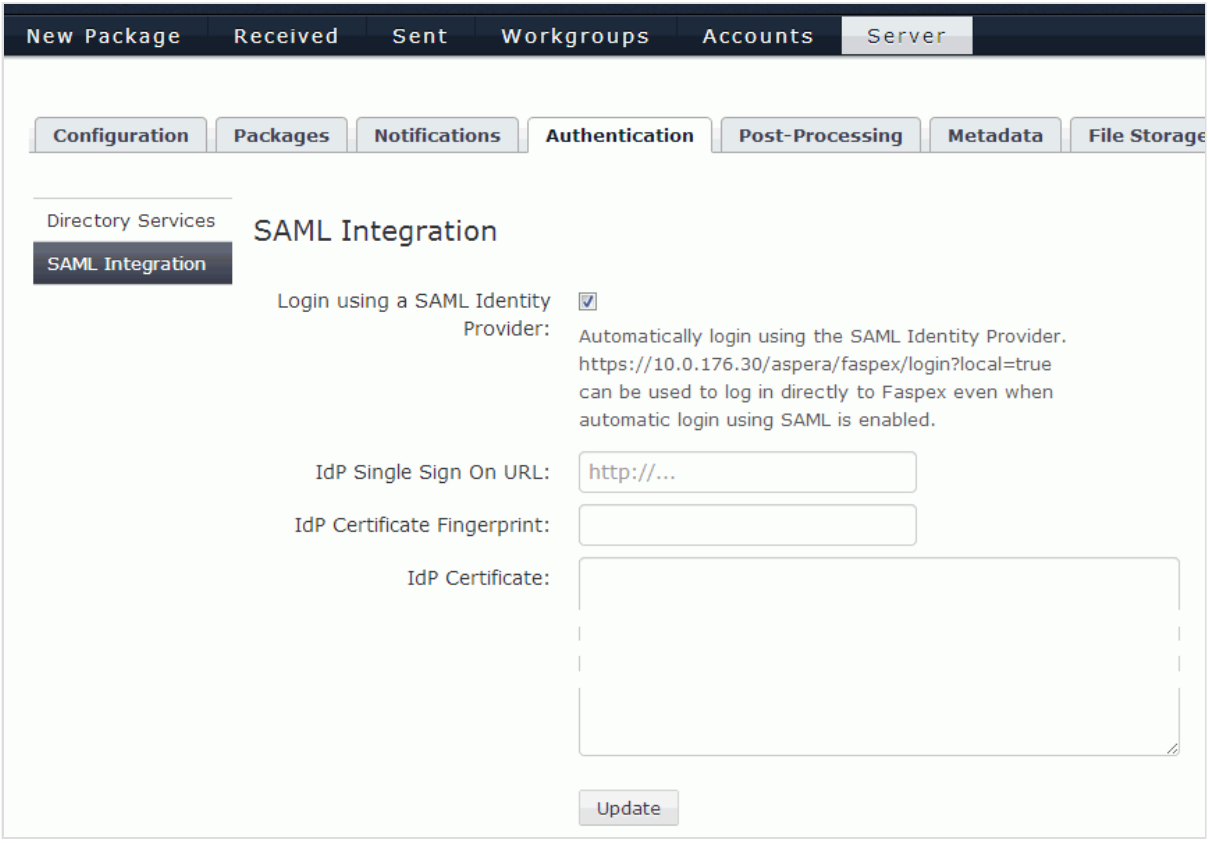
1. In Faspex, go to **Server > Authentication > SAML Integration**.

2. Check the box for “Login using a SAML Identity Provider”. The display expands with a form to fill in.

3. For “IdP Single Sign-On URL”, fill in the SAML entry-point address provided by the IdP.

4. In the fields just below, paste in either (a) the IdP Certificate Fingerprint or (b) the IdP Certificate.

5. Click **Update**.



A Faspex administrator can bypass the SAML login and sign in with the regular login form by adding the local=true parameter to the login URL, for example:

```
https://10.0.176.30/aspera/faspex/login?local=true
```

Setting up an Identity Provider

A Faspex admin setting up SAML needs to provide the following information to the IdP in order for the IdP to communicate with the Faspex server:

Name ID Format	`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
Entity ID	`https://www.`*`our-faspex-server`*`.com/aspera/faspex/`**`auth/saml/metadata`**
Binding	`urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`
Callback URL	`https://www.`*`our-faspex-server`*`.com/aspera/faspex/auth/saml/callback`

The above data can be retrieved directly from **auth/saml/metadata** if the IdP is capable of reading SAML XML metadata for a service provider.

Faspex expects assertion messages from an IdP to contain the following elements:

Element	Format
`SAML_SUBJECT`	`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

Element	Format
email	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
given_name	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
id	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
surname	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Post-Processing

Add post-processing scripts to run on package receipt.

Faspex administrators have the ability to execute post-processing scripts on the server to accomplish tasks such as virus checking, moving files, and creating backups once packages arrive. Post-processing uses a set of filtering options to determine when to execute customized scripts. Faspex can execute shell scripts and Windows batch scripts, where information about the package is passed to the script by means of environment variables.

Post-processing scripts that have been activated execute automatically after the initial transfer to a default inbox. The relay of a package to a custom inbox does not trigger script execution.

IMPORTANT NOTE: In the event that a Faspex Administrative account is compromised, post-processing can be a serious threat to your server's security. Thus, Aspera strongly recommends that you update your administrative users' permissions in order to prevent unauthorized users from executing post-processing on your Faspex server. To secure your Faspex server, follow the instructions described in *Configure a Secure Faspex* on page 24. *Note that by default, post-processing is enabled. To disable it for security reasons, please see the instructions at the end of this topic.*

To prepare a post-processing script, follow the steps directly below.

1. Prepare the post-processing script

   Generate your post-processing script and place it in a directory on the machine running your Faspex server. Take note of, or copy, your script's full system path on the server. You can utilize the following environment variables in your post-processing scripts, but be sure to use the proper format. For example, the variable *faspex_pkg_directory* will be available as *$faspex_pkg_directory* in shell scripts, and *%faspex_pkg_directory%* in Windows batch files.

Variable	Description
faspex_pkg_directory	Storage directory of the package. See cautionary note below.
faspex_pkg_name	Package title.
faspex_pkg_note	Package note.
faspex_pkg_id	Package ID.

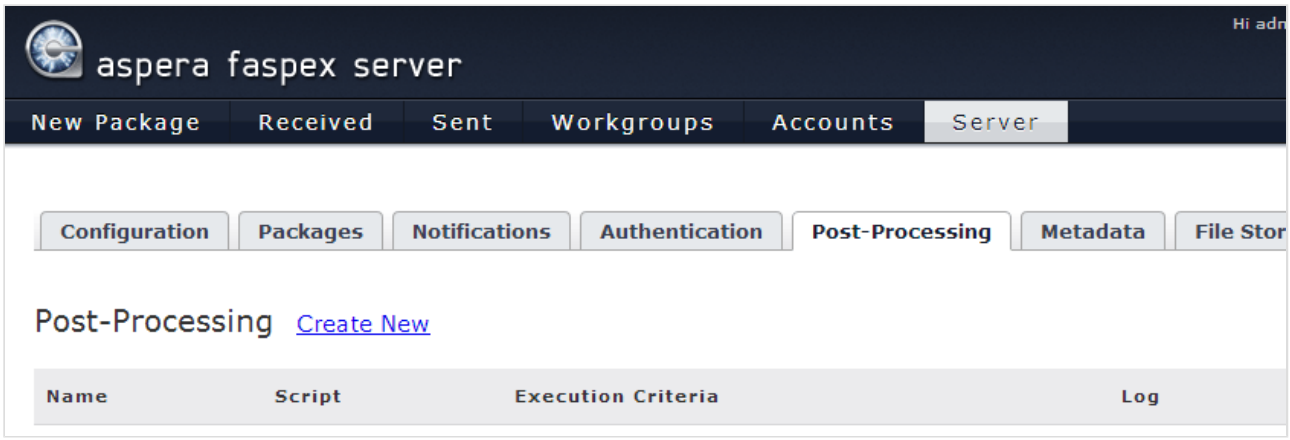
Variable	Description
faspex_recipient_list	Comma-separated list of recipients. (e.g. "admin, johndoe")
faspex_recipient_count	Number of recipients. (e.g. "3")
faspex_recipient_i	Name of the recipient. (i starts at "0", e.g. faspex_recipient_0, faspex_recipient_1 ...)
faspex_sender_id	The sender's ID.
faspex_sender_name	The sender's full name.
faspex_sender_email	The sender's e-mail.
faspex_pkg_total_bytes	Size of the package in bytes.
faspex_pkg_total_files	Number of files in the package.
faspex_pkg_uuid	The package's UUID (36 characters).
faspex_metadata_fields	Comma separated list of the metadata fields defined for the package
faspex_metadata_<field>	The value of the metadata field named <field>. In the field name, spaces are converted to underscores, non alphanumeric characters or underscores are stripped. For example, "my field" becomes "my_field"; "*my_group" becomes "mygroup".

CAUTION: If you are upgrading from Faspex 2.X to 3.X and use post-processing scripts, you will need to modify the scripts as follows, since the package's full path is no longer available to the scripts:

- If the transfer server is on the same machine (node) as Faspex, ensure that the package path is prefixed with the Faspex user's docroot. After doing so, you may want to check for an extra "**/**" character in the path if you have a "**/**" both at the end of the docroot and at the start of the path as defined in **$faspex_pkg_directory**. For example, the entry **/home/faspex/faspex_packages/$faspex_pkg_directory** and a package title of "NewVideos" could result in **/home/faspex/faspex_packages//NewVideos - 10d8a2f1-30f4-47ad-a55b-6f8dbba7ff8d/PKG - NewVideos**.
- If the transfer server is on a different machine, modify post-processing scripts to invoke the Node API, or mount the remote volume on the Faspex server.

2. Set up post-processing within the Faspex Server GUI

   Go to **Server** > **Post-Processing** and click **Create New**.



In the *Add New Script* screen, enter the following information. Click **Create** when finished:

Script to run

Item	Description
Name	A descriptive name for this script.
Path to script on server	Enter the full path to the executable script that exists on the server. **IMPORTANT NOTE:** The System user **Faspex** should have the proper permissions to access and execute this file.
Active	Check to enable this script.

Execution criteria

All specified criteria must match the uploaded package's attributes for the script to be run on that package. All match fields in this section are optional. When **Exact match** is checked, the package attribute has to match the specified criterion exactly for the script to be run, the entered text will be matched anywhere in the field.

Item	Description
Package name	Execute when the package name matches the string.
Sender name	Execute when the sender name matches the string.
Sender email	Execute when the sender email matches the string.
Recipient name	Execute when the recipient name matches the string.
Recipient email	Execute when the recipient email matches the string.
Package note	Execute when the package note matches the string.
Package date	Execute when the package date falls into the determined range.

Item	Description
Package size	Execute when the package size falls into the determined range.
Package file count	Execute when the package file count falls into the determined range.

For security reasons, you may optionally disable post-processing in *faspex.yml*. The *DisablePostProcessing* setting can be found in the *faspex.yml* file, accessible via the following path:

OS Version	Location
Windows 32-bit	C:\Program Files\Aspera\Faspex\config\faspex.yml
Windows 64-bit	C:\Program Files (x86)\Aspera\Faspex\config\faspex.yml

IMPORTANT NOTE: Aspera strongly recommends backing up *faspex.yml* before modifying.

Within faspex.yml, change "DisablePostProcessing:false" to "DisablePostProcessing:true"

```
...
DisablePostProcessing:true
...
```

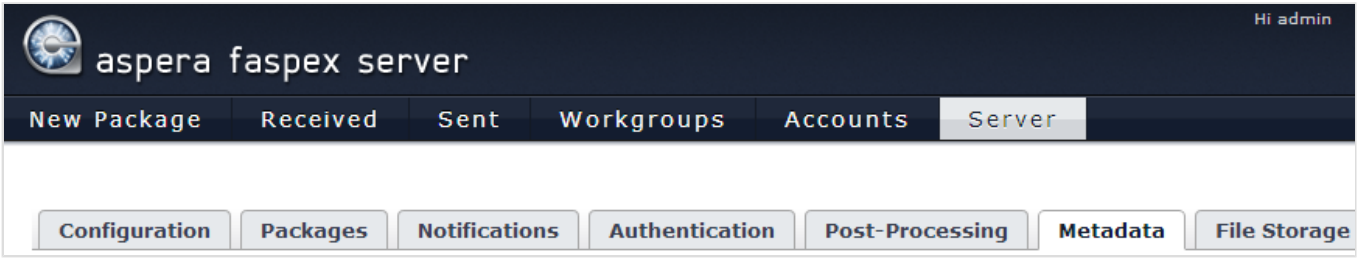
Metadata

Adding Metadata fields in the send form.

Metadata refers to the additional information that a user can send with a file package. For example, when a user sends an audio-file package to his producer, he is required to specify the sample rate, bit depth and compression. In this case, the sample rate, bit depth and compression represent a package's *metadata*. The "Submit Package" form can be easily configured to include input fields for sample rate, bit depth and compression. To do so, we must set up a *metadata profile*. The *metadata profile* contains your metadata fields. To continue this example, we'll be setting up a metadata profile to capture key information for this audio file. The profile *Audio Details* will contain the following fields:

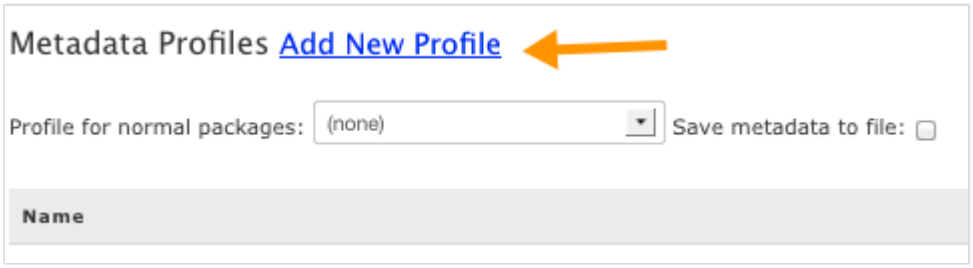
- Sample rate (text input field)
- Bit Depth (option list that includes 8-bit, 16-bit and 24-bit)
- Compression (text input field)

To create, view and edit metadata profiles, start by going to **Server** > **Metadata** . As an Administrator, you can designate which metadata profile each Dropbox's "Submit Package" page will use, as well as which profile the normal "New Package" page will use. Admins can also elect to assign "(none)" as a metadata profile in cases where no metadata fields are desired.

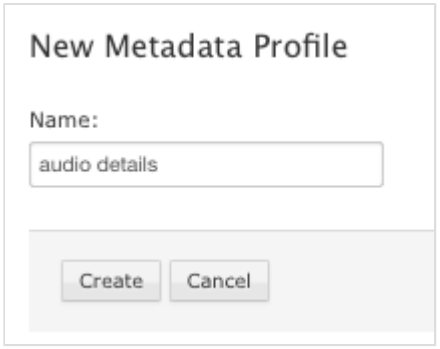


On the *Metadata Profiles* page, any profiles that you have previously created will be available under the **Profile for normal packages** drop-down list.

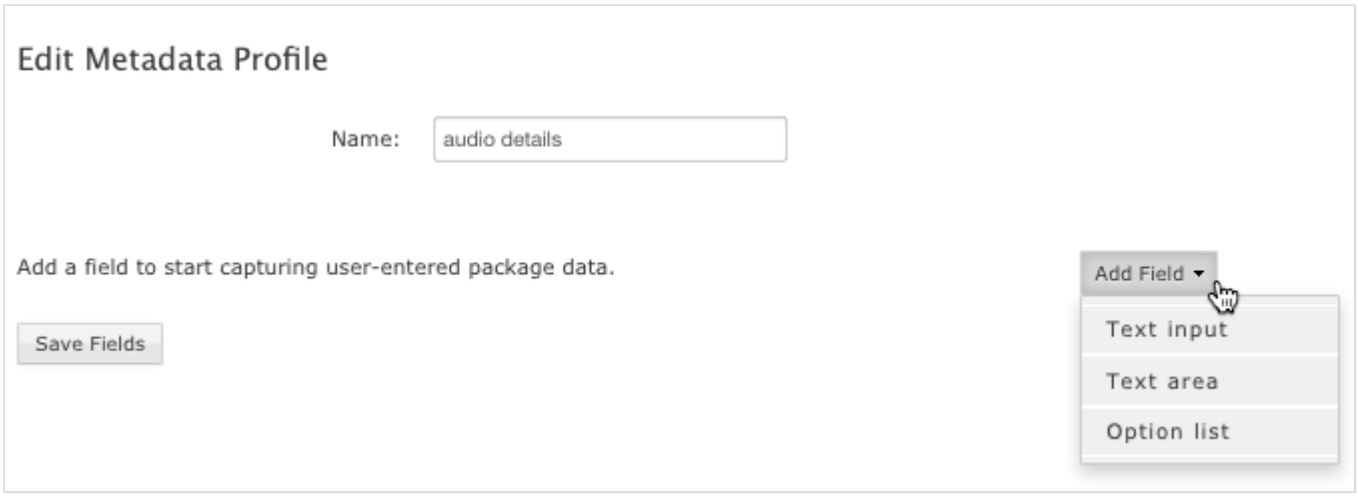
1. To create a new profile, click the **Add New Profile** link.



2. Name your new profile and click the **Create** button.



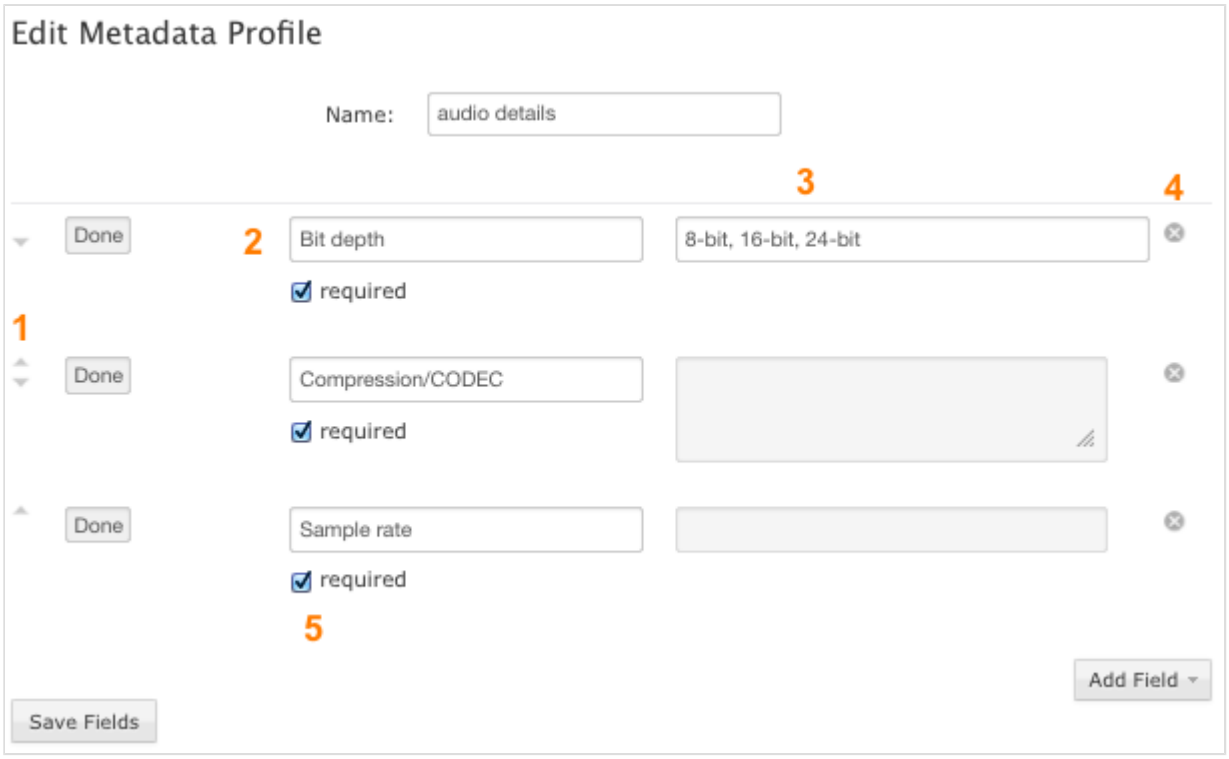
Once you have clicked **Create** button, you will be prompted to select the metadata type from the **Add** drop-down list. Select **Text input** to create a single-line text field, **Text area** to create a multi-line text field and **Option list** to create a radio button-based options list.



NOTE: You can add more than one metadata field.

3. Modify the field template

Each field option has a template associated with it. Using the template, you can modify a field's label and, for the Option list metadata field, its options. Once the template appears, click the **Edit** button to launch edit mode.



#	Description
1	Use the arrows to re-order multiple metadata fields.

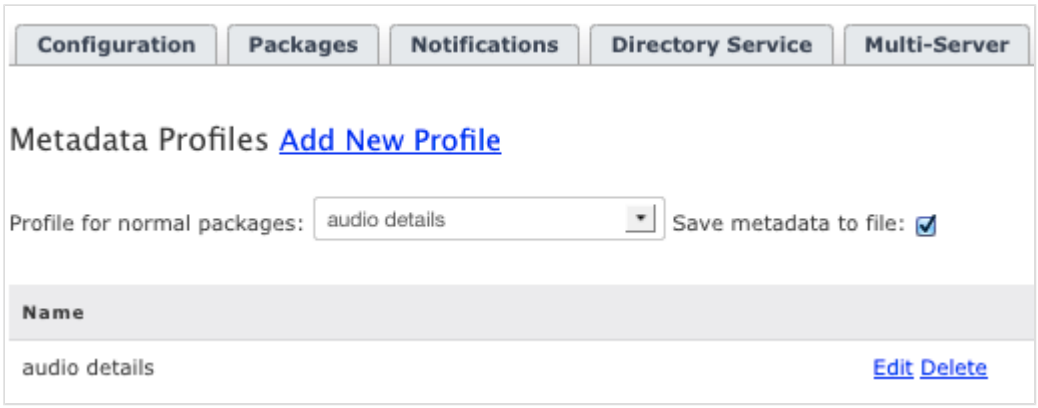
#	Description
2	Enter the metadata field's label. This label will appear next to the field on the send form.
3	If this is an options list, enter multiple options that are separated by commas (,).
4	Use the "x" icons to delete fields.
5	If the field is required, check **Required**.

4. When finished editing your metadata field(s), click the **Done** button next to the corresponding field and then click **Save Fields**.

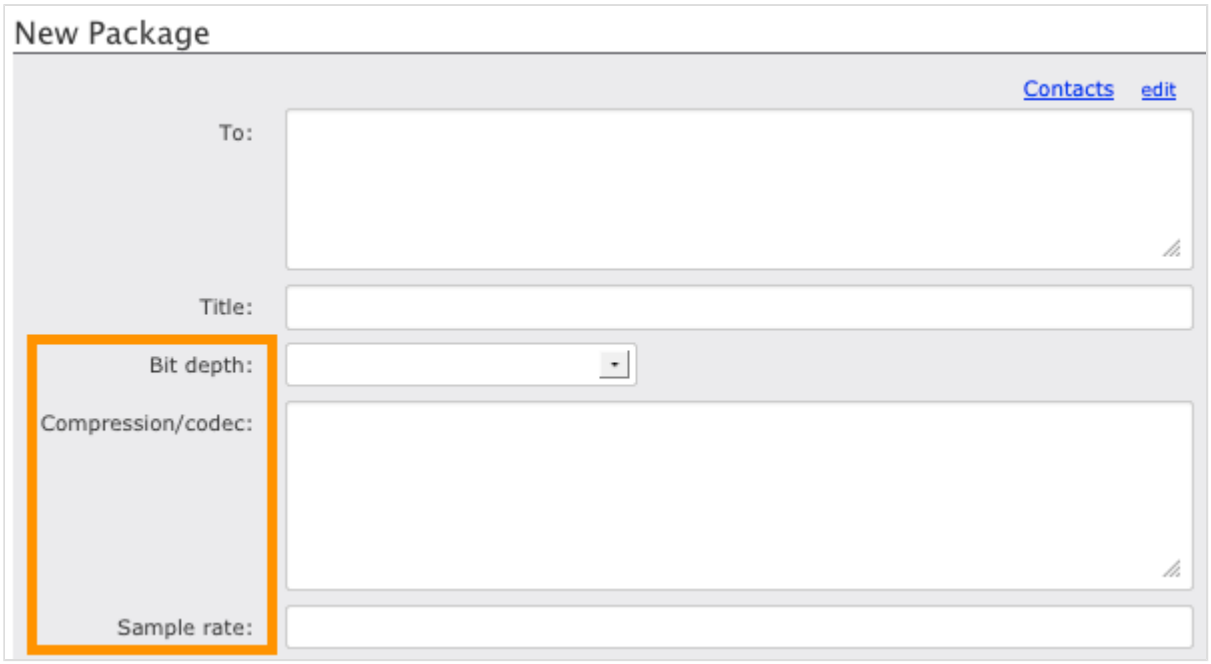
You will now see the new metadata profile listed on your *Metadata Profiles* page (along with any other profiles that you have created). From here, you can perform the following functions:

- **Edit** your profile
- **Delete** your profile
- Select a profile as your normal packages default metadata template (via the **Profile for normal packages** drop-down list).

You can also enable the **Save metadata to file** checkbox. When enabled, the package's metadata is saved to its root directory in the file `aspera-metadata.xml`. You can use the XML data for post-processing and automation.



When sending a **normal package**, you will see the new metadata fields on the *New Package* page.



NOTE: When you forward a package (normal or dropbox), the original metadata is preserved in the note, even as new metadata fields from the current profile are available. However, even if "Save metadata to file" is enabled, no new `aspera-metadata.xml` is created.

Faspex can also be configured so that the metadata file is included inside the package itself, instead of being placed at the root directory of the package. To enable this, set the **SaveMetadataInPackage** option to true in the configuration file `faspex.yml` as follows:

```
...
SaveMetadataInPackage:true
...
```

The *faspex.yml* file is located in the following directory:

OS Version	Location
Windows 32-bit	C:\Program Files\Aspera\Faspex\config\faspex.yml
Windows 64-bit	C:\Program Files (x86)\Aspera\Faspex\config\faspex.yml

Then, whenever the **Save metadata to file** checkbox is enabled, `aspera-metadata.xml` will be inserted in packages, and it will be visible when the package contents are viewed in Faspex.

File Storage

Manage your remote file storage for Faspex.

Faspex Server v3.X supports remote file storage, which means that senders can create packages with files that are stored on another server, as well as on their local machines. Before v3.X, senders were only able to browse their local machine for files to send through Faspex. Remote file storage can also be used for inboxes, i.e., locations where packages can be received.

IMPORTANT NOTE: Only *registered* Faspex users (i.e., those you have created accounts for within Faspex or imported from DS) can browse remote file storage. Outside senders are not permitted to access remote file storage. Additionally, *every* registered Faspex user can access *all* file storage (meaning that you cannot limit file storage access to certain registrants); however, a registered Faspex user cannot *send* from remote sources unless their account is configured with **Create packages from remote sources** enabled and their permission settings give them access to the source.

Configuring Faspex to Communicate with your remote Enterprise Server Node

To configure Faspex to communicate with a remote node:

1. **Ensure that Enterprise (or Connect) Server v3.0+ is installed on the node machine.**
2. **Have the following information readily available:**
   - **The node computer's hostname or IP address, along with a port and path (if applicable).**
   - **The node API username and password, which you created when you set up Enterprise Server on your node machine.**

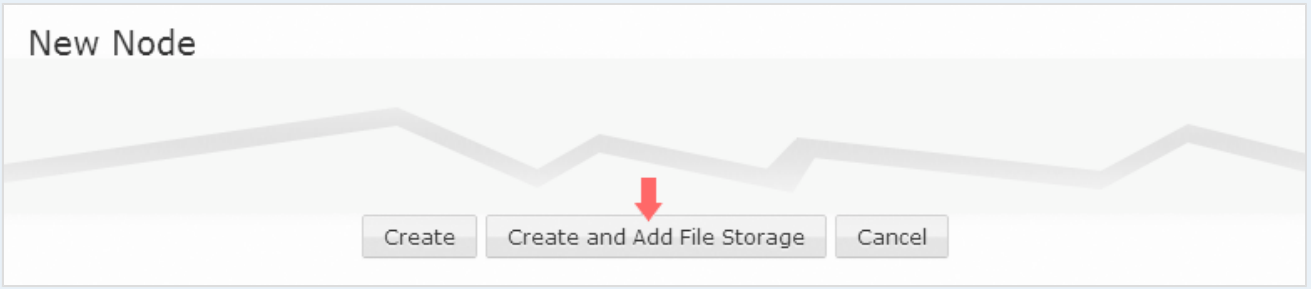
   If you do not have this information, please refer to the admin guide for Enterprise Server or Connect Server v3.0+.

3. **See the instructions for preparing a remote transfer-server node in *Setting up a Remote Server* on page 158.**
4. **Follow the instructions for adding the remote server to Faspex, in *Transfer Server* on page 43.**

Adding/Browsing the File Storage on your Remote Server

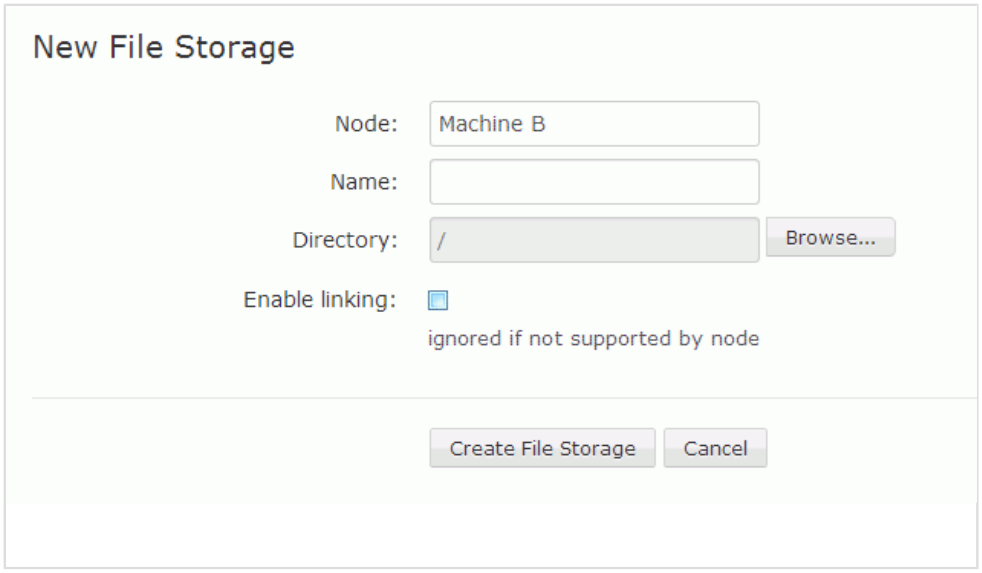
You can add file storage to a node in either of two ways:

- When you originally create the node (see *Transfer Server* on page 43) click **Create and Add File Storage**.

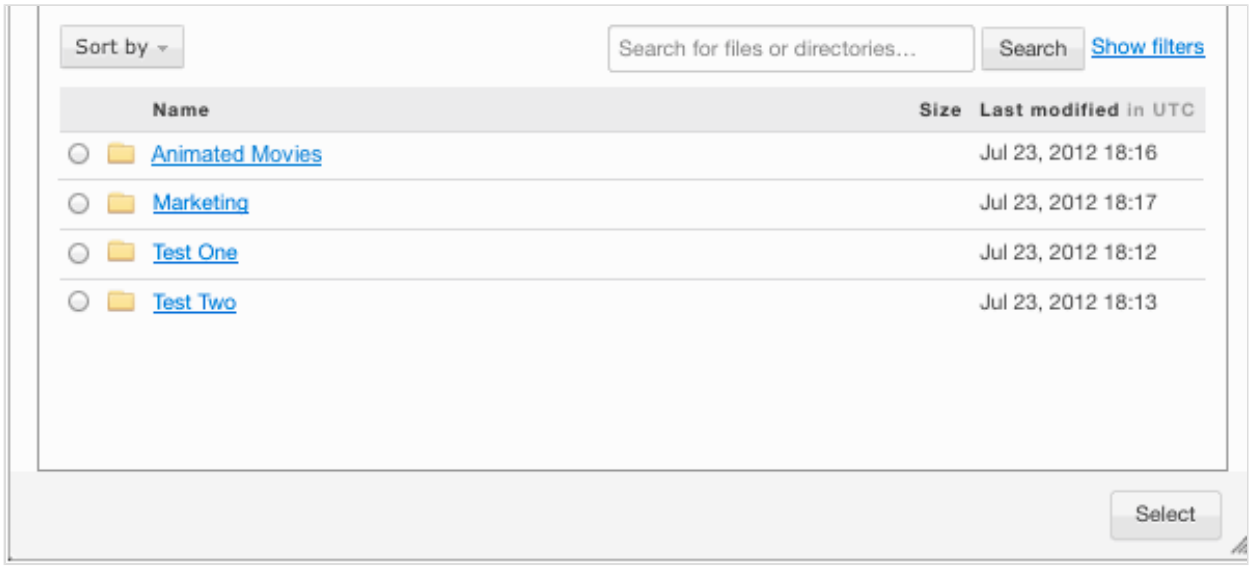


- By adding it to a node you have already created. (See *Modifying a Node and Adding File Storage* on page 102 below.)

Either choice opens the New File Storage dialog which lets you browse for and select the file-storage directory.



When you click the **Browse...** button, you are prompted to select a directory in the pop-up window. Note that you will only be able to browse within the docroot that was associated with your transfer service user and API username. In the above example, the directory "/" means the docroot, not the root of the server node's file system.

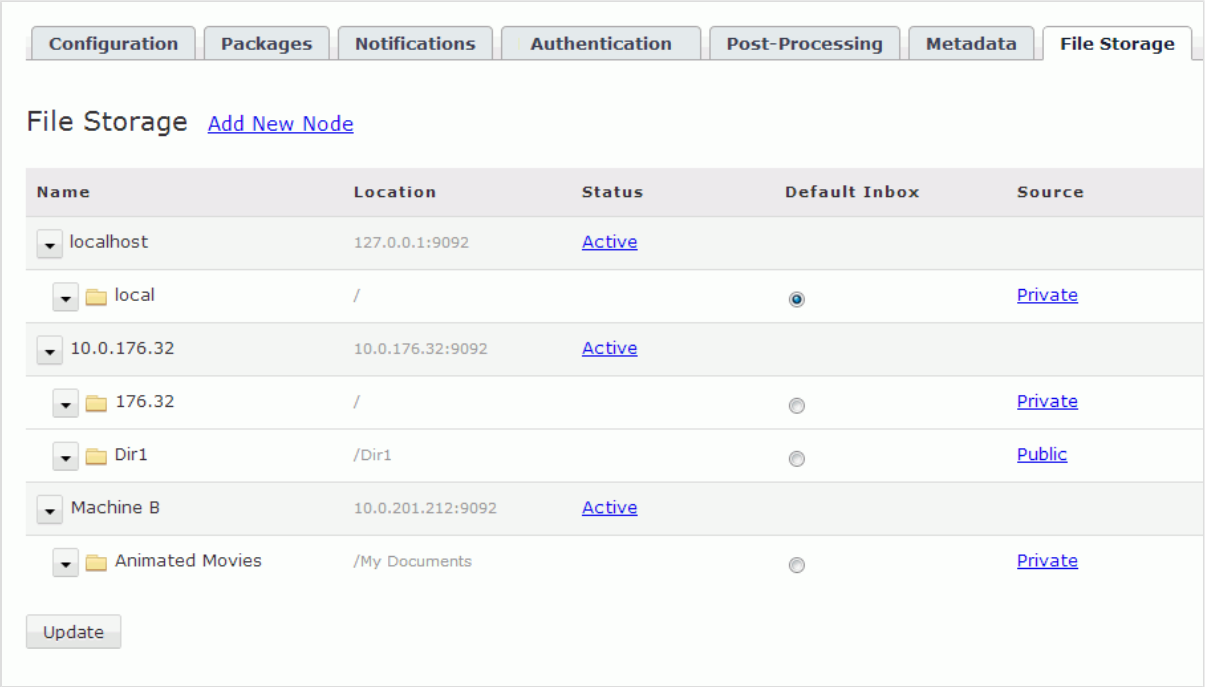


Here, you have several options:

- You can perform a simple search for a directory by entering it into the name field and clicking **Search**.
- You can perform an advanced search by clicking the **Show Filters** link, and entering your criteria.
- You can sort the directory list by type, size, size descending, last modified, and last modified descending.
- You can select a radio button next to the directory that you would like to be the share. After clicking the radio button, click **Select**.

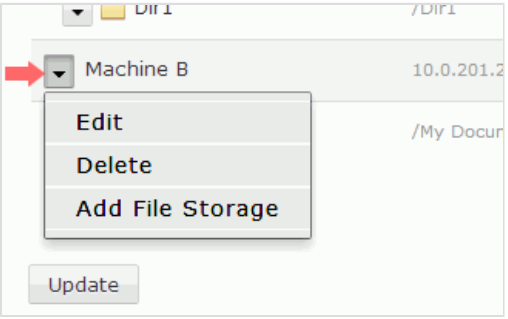
Once you have selected your file storage on the node, click **Create File Storage**. You should now see your node and file storage listed on the *File Storage* page For each node, the display shows its name and its status (active or error). The **Active** and **Error** links provide more detail on status. The display indicates which location is the current default inbox, and the permission level for access to sources in that location (private, public, or limited). By default, source directories are created with the private level. For information about what the permission levels mean and how to change them, see *Modifying File Storage and Setting Access Permissions for Source Directories* below.

In a fresh install, the default inbox is **packages**. You can change the default inbox to any file storage directory on an active node by clicking one of the option buttons in the Default Inbox column. If the node's connection status is **Error**, the option button will be grayed out and not selectable. When you are finished selecting a different location for the default inbox, click **Update** at the bottom of the display to save your selection.



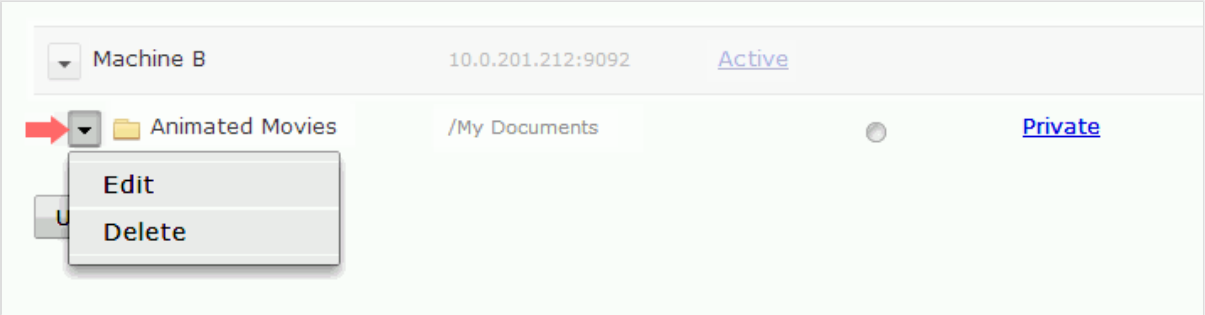
Modifying a Node and Adding File Storage

To modify or remove a file storage node, or add storage directories to it, click the down-arrow icon in front of its name. Clicking **Edit** opens the *Edit Node* page which, except for the title, is the same as the *New Node* page (see previous section), and offers the same modification choices. Clicking **Delete** removes the node from your file storage. Clicking **Add File Storage** opens the *New File Storage* page (see previous section).



Modifying File Storage and Setting Access Permissions for Source Directories

To modify or remove a file storage directory, click the down-arrow by the directory name. Clicking **Delete** removes the directory from your file storage (however, it does not remove the directory from the node's disk). Cllicking **Edit** opens the *Edit File Storage* page, from which you can modify the directory or set sosurce access permission. You can also reach the *Edit File Storage* page by clicking the links for **Private**, **Public**, and **Limited**.



The *Edit File Storage* page lets you modify the following settings for a file storage directory:

- **Name** - change the Faspex name for the storage directory.
- **Directory** - associate the Faxpex name with a different directory in the node's file system.

NOTE: The Node field cannot be changed on the *Edit File Storage* page. It can only be modified from the *Edit Node* page.

In addition, you can set or modify the following:

- **Enable linking** - enable files that are sent from this location to be copied to the inbox as symbolic links (symlinks). Both the default inbox and the source location of the files must be on the same node. If they are not on the same node, checking this box has no effect.

  NOTE 1: Packages sent to a workgroup or dropbox with a custom inbox will not be symlinks. The default inbox will contain symlinks, but custom inboxes will contain actual files.

  NOTE 2: The linking feature does not work if the Enterprise Server node or the file-storage node is a system that does not support symbolic linking.

  NOTE 3: Enabling linking is ignored if EAR is enabled.

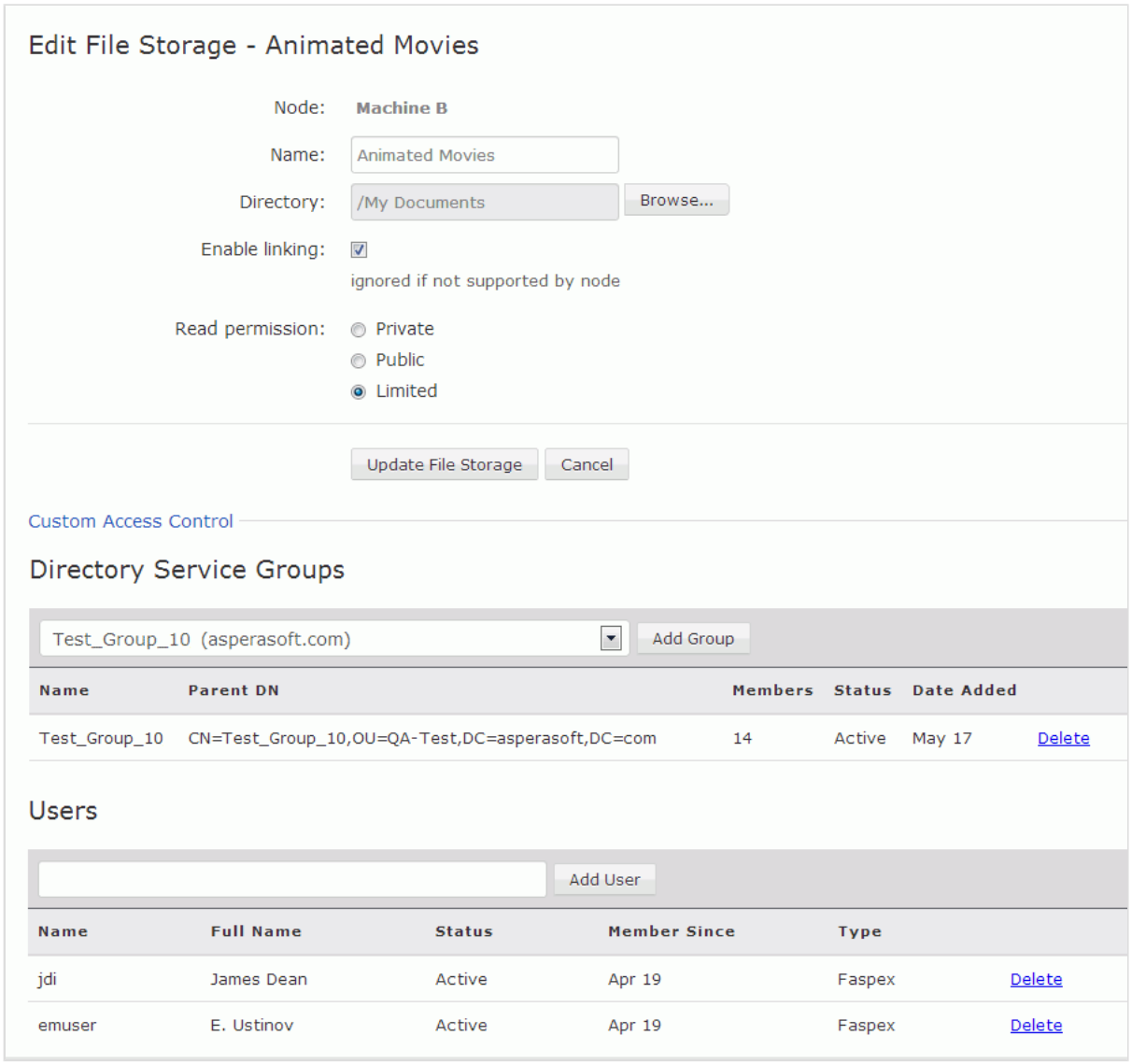
- **Read Permission** - set permissions for this source location as follows:

  Private - (Default) No users can send content stored in this location. (However, even if private, this location can still serve as inbox storage.) Note that enabling linking (checking the **Enable linking** box) is not relevant for sources that are private.

  Public - Any user can send content stored in this location (as long as their account is configured to allow it).

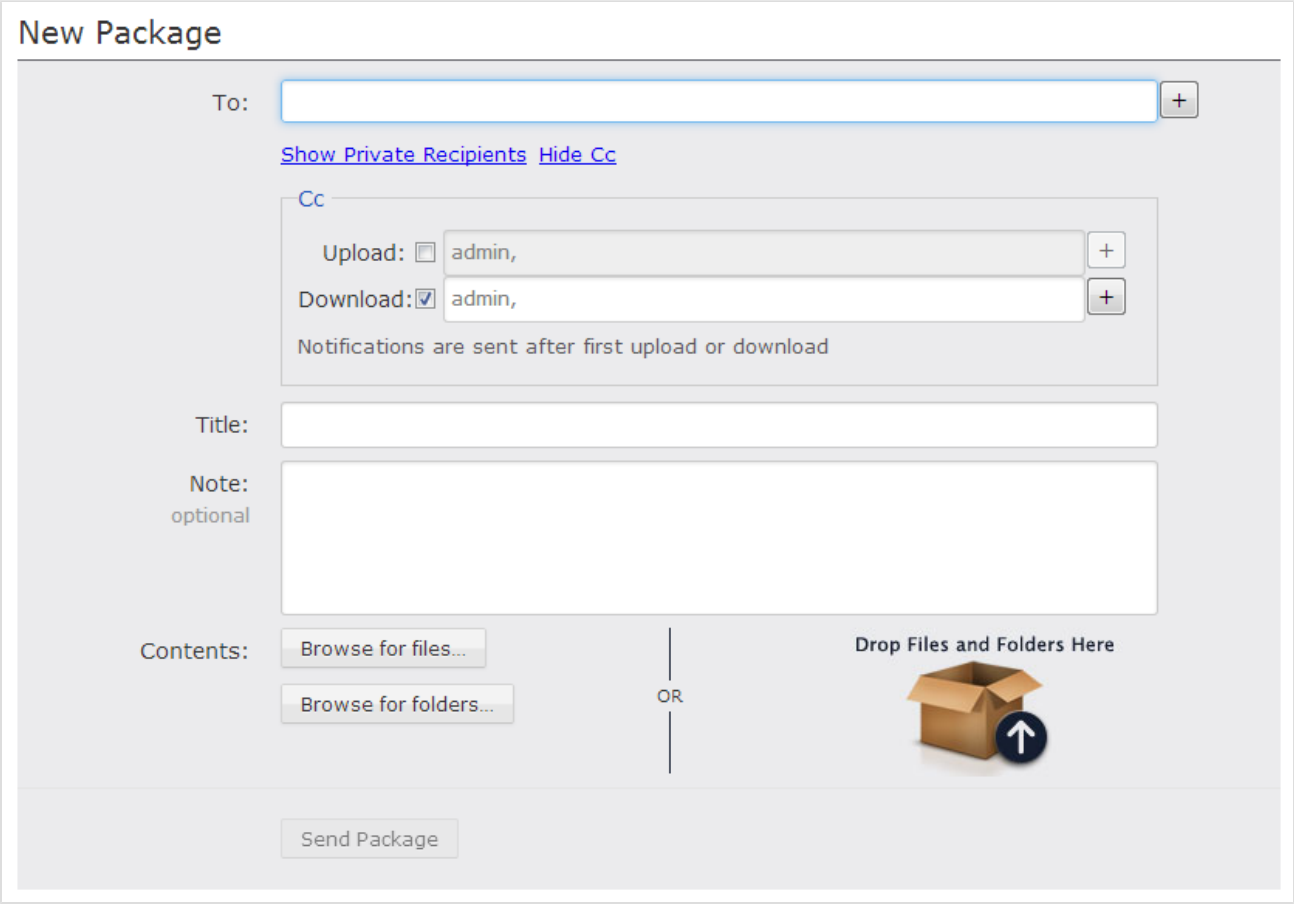
  Limited - Only certain users can send content stored in this location (as long as their account is configured to allow it).

When **Limited** is selected, the *Custom Access Control* display appears, allowing you to specify which users or DS groups can send content stored in this location. (DS groups can be added only if directory services is enabled in **Server** > **Authentication** / **Directory Services** .) Add users and DS groups one at a time; comma-separated lists are not allowed. Note that workgroups cannot be specified here, only DS groups and individual users.



Selecting a File Source when Creating a New Package

Now that you have a file storage set up, registered Faspex users can select and browse it when creating a new package (in addition to browsing for a file on their local computers).



Advanced Config Options

Additional configuration options (via faspex.yml).

This topic covers additional Faspex configuration options that can be applied via *faspex.yml*. These options including the following:

- Hidden Directory Service (DS) features.
- Hidden password settings.
- Hidden self-registered users settings.

Remember, editing *faspex.yml* is for advanced, administrative users only! To access *faspex.yml*, go to the following directory:

OS Version	Location
Windows 32-bit	C:\Program Files\Aspera\Faspex\config\faspex.yml
Windows 64-bit	C:\Program Files (x86)\Aspera\Faspex\config\faspex.yml

IMPORTANT NOTE: Be sure to back up faspex.yml before modifying!

The following tables describe hidden Faspex options, along with their default values.

Directory Services

Item	Description	Default
DsUsernameAttribute	Specifies the DS attribute to use as the Faspex username. The chosen attribute should be unique. Note that this option should be set before importing any DS users and should not be changed afterwards. Examples: mail, samaccountname (Active Directory).	Depends on attributes returned by directory service
DsSyncPeriod	Specifies how much time must pass since the last synchronization operation in order for a group or user to be judged in need of another.	3600 *(seconds)* / 1 hour
DsCheckPeriod	Specifies check period for synchronization operations. It is during these checks that the DsSyncPeriod parameter is used to determine if synchronization is necessary.	600 *(seconds)* / 10 minutes
DsSyncActiveState	Determines whether to sync, or not. Valid values: true, false.	true
CanonicalizeLdapGroupMemberSearch	Causes Faspex to strip spaces out of DNs during comparisons that may prevent Faspex from properly identifying DS users. Should only be set to true if it is proven that your LDAP server is returning DNs with inconsistent spacing (e.g. inserting or omitting spaces when user info is queried as part of an LDAP group vs. individually). Valid values: true, false.	false

Password

Item	Description	Default
StrongPasswordRegex	A regular expression that can be used to customize strong password requirements. Changing this setting will not affect existing passwords, but any new password must match	(?=.*\d)(?=.*([a-z]|[A-Z]))(?=.*(\W|_)).{6,}

Item	Description	Default
	with this regular expression. Example: (?=.*[A-Z])(?=.*(\d|\W|_)).{7,}	
StrongPasswordRequirements	A description of the strong password requirements. Should match the regular expression specified by StrongPasswordRegex. Example: “must be at least seven characters long, with at least one capital letter and one number or symbol.”	“Must be at least six characters long, with at least one letter, one number, and one symbol.”

Self-registered Users

Item	Description	Default
EnforceSelfRegisteredUserEmailUniqueness	Prevents registering for an account using an email address that is already used by a full Faspex user (i.e. not merely in use by an external email user record). Valid values: true, false.	false (not enforced)
SelfRegistrationUsesEmailAsLogin	Forces self-registering users to choose a login name that is in the format of an email address. Note that this makes entering email address redundant but it is still required. Valid values: true, false.	false (not enforced)

Metadata

Item	Description	Default
SaveMetadataInPackage	Whenever this option is set to "true" and the **Save metadata to file** checkbox is enabled on the Metadata Profiles page, the Create New Dropbox page, or the Edit Dropbox page, the metadata file `aspera-metadata.xml` is included inside packages, instead of being deposited in a package's root directory.	false

User Management

Create and manage Faspex Users

Creating a New Faspex User

Creating local, non-Directory Service, Faspex user accounts.

You can create new Faspex user accounts and edit associated permissions via the *Accounts* menu option. When creating and editing Faspex user accounts, you can modify the following permissions:

- Receive packages
- Forward packages
- Send packages to workgroup members
- Send packages to all Faspex users
- Send packages to external email

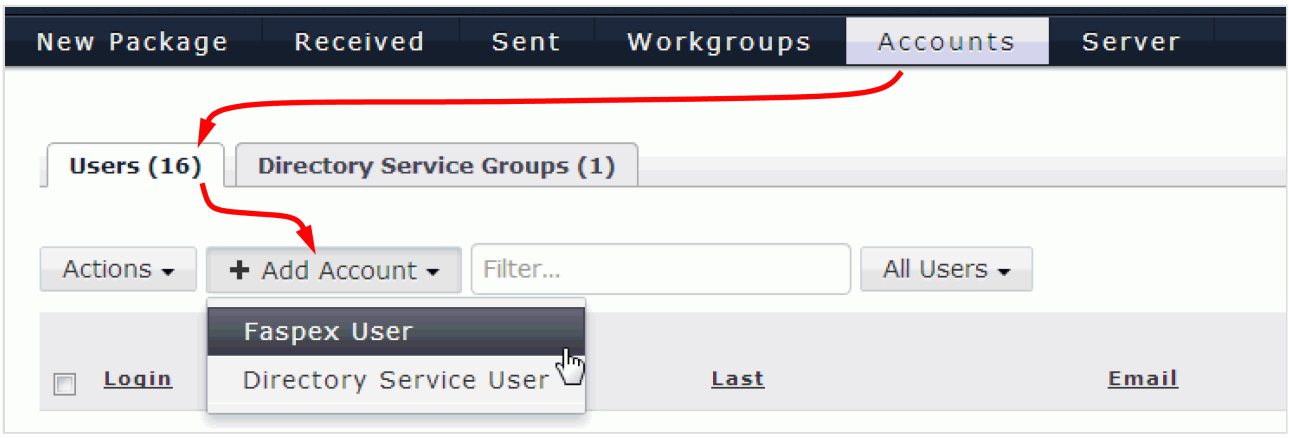
This topic demonstrates how to create local, non-directory service, Faspex user accounts.

IMPORTANT NOTE: For information on adding directory service users or groups, see the topic *Authentication: Directory Service* on page 77.

IMPORTANT NOTE: You can make certain fields required within the *New User Account* form. For details, see *Customizing New-User-Account Form* on page 137\.

Add Faspex accounts

To create a new Faspex user account, click the **Accounts** tab and select **Add Account** > **Faspex User**.



Within the *New User Account* screen, enter the following information:

Item	Description
Login	The user account's login.
Password	The user account's password. Note that you can enforce the creation of strong passwords. Please refer to *Security* on page 56 for additional information.
Confirm Password	Confirm the user account's password.
E-mail	The user's email address (where Faspex Server notifications will be sent). Please refer to *Notifications* on page 68 if you would like instructions on modifying Faspex Server's email templates.
First Name	The user's first name.
Last Name	The user's last name.
Edit settings and permissions	Click this link to reveal additional user settings (refer to the following section for details).

The following section covers all options within the **Edit settings and permissions** screen. When finished the configuration, click **Done**.

Account Options/Details

Option	Description
Password expires	Enable if you would like the user's password to expire every specified number of days.
Role	Select from one of the following roles for this user: • **Administrator** - Administrators can access the **Server** tab to configure the Faspex server. They can create, edit, and delete every type of Faspex user (administrators, managers, and regular users), and they can send packages (perform file transfers). Administrators can also manage workgroups (create/edit/delete). • **Manager** - The manager role enables Faspex server administration to be separate from Faspex user accounts administration. Managers can send packages, create/edit/delete workgroups, and create/edit/delete other managers and regular users. They can promote regular users to managers, and demote other Managers to regular users. However, they cannot, edit administrator accounts or promote another user to administrator. Managers do not have access to the **Server** tab, nor can they change the Faspex server configuration (a privilege limited to administrators).

Option	Description
	• **User** - Regular users can send packages through Faspex. They typically do not manage other users or workgroups. • **Workgroup Administrator** - NOTE: The workgroup administrator role is assigned and managed under the Workgroup view, not from the Accounts view. For details, see *Create and Manage Workgroups* on page 121. A user can be designated as a "workgroup administrator" (by a Faspex administrator or manager). Workgroup administrators manage specific workgroups according to the permissions set for that role in that workgroup.
Account expires	Enable if you would like this account to expire on the specified date.
Account activated	Enable to activate this account (i.e. turn on the account so that the user can log into Faspex).
Send copy of receipt email to these addresses	Enter email addresses that should receive a copy of the user's Faspex notifications. If you are adding multiple email addresses, separate them with commas (,), semicolons (;) or white-spaces.
Send a welcome email	Enable if you would like a Faspex welcome email to be automatically generated and sent to the user. Please refer to *Notifications* on page 68 if you would like instructions on modifying Faspex Server's email templates.
Show password in welcome email	Enable if you would like to include the user's password in the welcome email.
Additional comments for welcome email	Within this text box, you may append additional comments to the standard Faspex welcome email (specifically for this user).

Permissions

Option	Description
Upload Packages	Enable to allow the user to send file packages.
Download Packages	Enable to allow the user to download packages that have been received. A user who does not have this marked will still receive packages, but will not be able to download the files.
Forward Packages	Enable to allow the user to forward received file packages to other users. The package will be made accessible to the forwarded users within their Faspex accounts.
Create packages from remote sources	Enable to allow user to create a package from a remote source (i.e. a remote server, which is configured via **Server** > **File Storage**). Note that this setting is OFF, by default, and that it must be set on a per-user basis (i.e. there is no global option).

Option	Description
Allow inviting external senders	When enabled, external senders (those who do not have Faspex accounts) can be invited to send a package. Changing this user setting overrides the system default (set under *Security*).
Allow public submission URLs	A Public URL can be used by external senders to submit packages to registered Faspex users. The benefit of using a Public URL is in the time-savings, such that external senders no longer need to be individually invited to submit a package (although that functionality still exists). When a Public URL is enabled and posted to an email, instant message, website, etc., the following workflow occurs: **1. The external sender clicks the Public URL.** **2. The sender is directed to page where he or she is asked to enter and submit an email address.** **3. A private link is *automatically* emailed to the sender.** **4. The sender clicks the private link and is automatically redirected to the Faspex-user package submission page.** **5. Once the package is submitted through the private link, the Faspex user receives it.** Thus, when the field **Allow public submission URLs** is enabled (e.g. set to `Allow`), the Public URL feature is turned on for this user. If set to `Deny`, then the feature is turned off for this user. Note that changing the user setting overrides the system default (set under *Security*). **IMPORTANT NOTE:** Even if the Public URL feature is enabled for a registered Faspex user, he or she can override the feature for their own account by going to **Preferences** > **Misc** > **Enable public URL** and disabling the checkbox.
Can send to external email	Enable to allow the user to send a download link to external emails addresses (which are not Faspex users).
Can send to all Faspex users	Enable to allow the user to send packages to all Faspex users (as opposed to only being able to send packages to the user's workgroup members).
Allowed IP addresses for login	Specify the IP address(es) that a Faspex user can login from to view his or her account. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).
Keep user directory private	When set to **Yes**, prevents a Faspex user (even if they have permissions to send to all Faspex users) from being able to see the entire user directory. Changing this user setting overrides the system default (set under *Security*).

Option	Description
Allowed IP addresses for download	Specify the IP address(es) that a Faspex user can login from to download packages. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).
Allowed IP addresses for upload	Specify the IP address(es) that a Faspex user can login from to upload packages. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).

Package Deletion

Options available **after downloading** a package:

Option	Description
Accept the system default	Follow Faspex Server's default auto-deletion settings. The current setting is displayed in the description. To update the default setting, refer to *Package Storage* on page 62.
Always use the following policy	Override the system default with the selected policy: • Do nothing • Delete files after **any recipient** downloads all files • Delete files after **all recipient** download all files
Allow user to set own delete setting on a package-by-package basis	Provide the policy settings in the user's **New Package** screen. The user can determine the file package's expiration rule when preparing it.

Advanced Transfer Settings

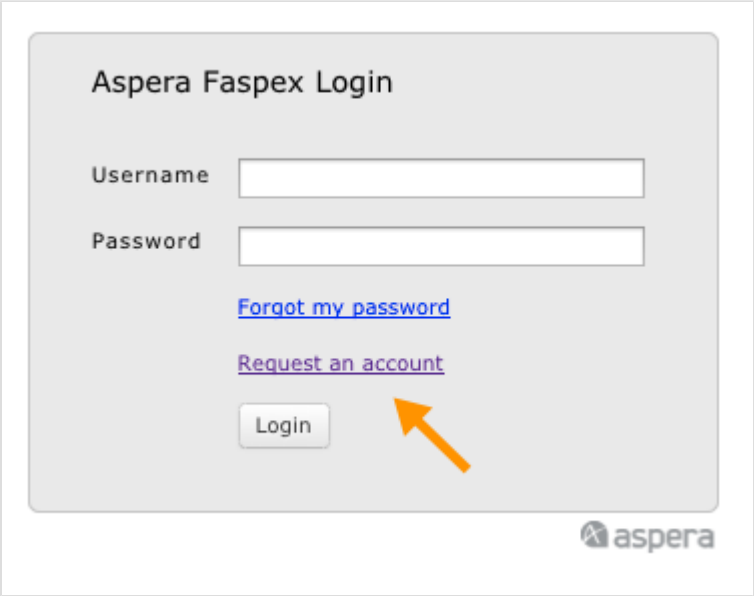
Faspex uses the transfer settings from the Aspera Central Server section by default. However, when **Override default settings** is checked, you can set user-specific transfer settings, which will take precedence over the server-wide settings.

Option	Description
Initial Transfer Rate	Specify the initial upload and download transfer rate. When the option **Lock minimum rate and policy** is checked, the user will not be able to adjust transfer policy or minimum transfer rate.
Maximum Allowed Rate	Specify the initial upload and download transfer rate.

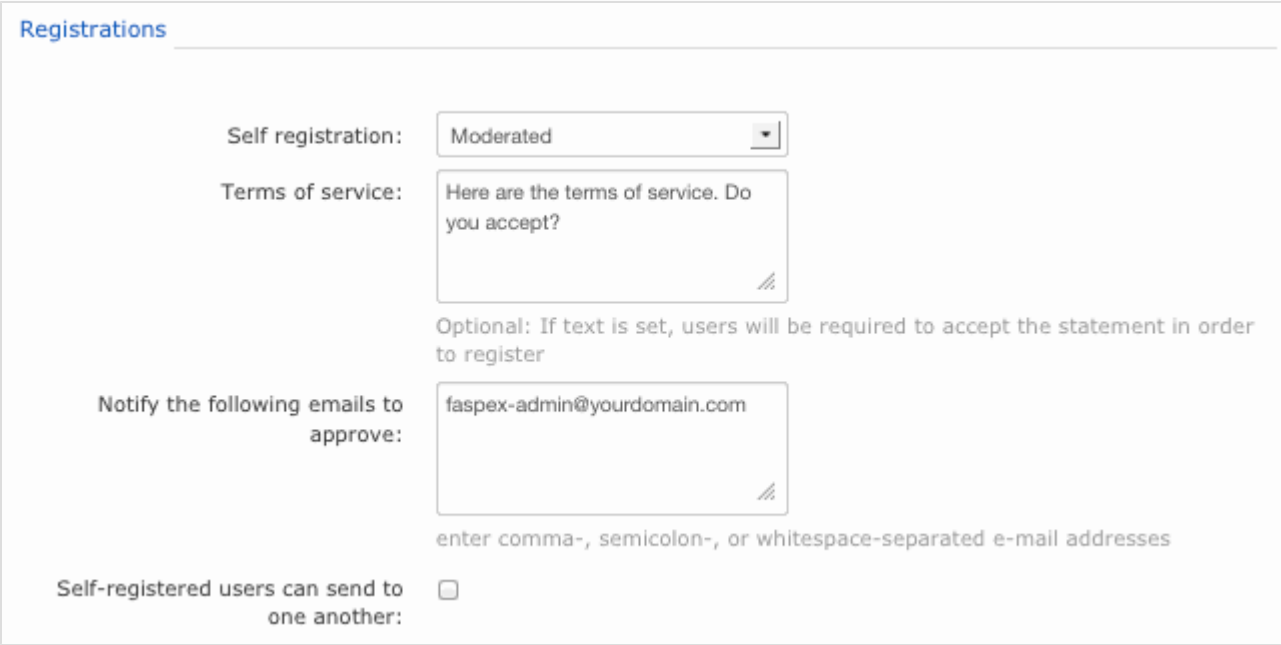
Self-Registered Users

Managing self-registered users and the template user.

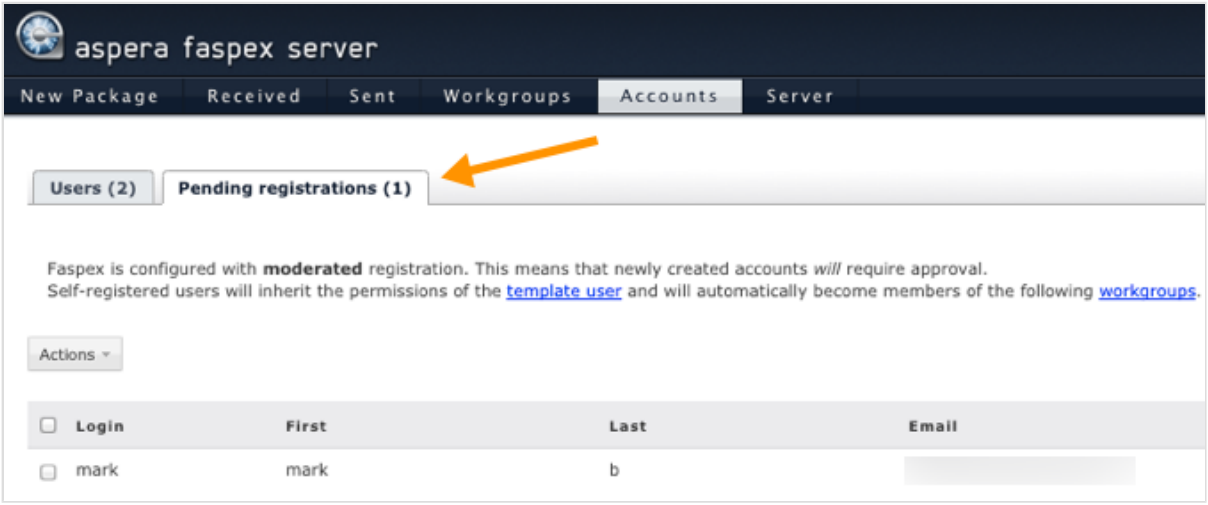
Faspex 3.X gives you the ability to allow non-registered users to request accounts on the Faspex login page. This relieves the workload of Administrators and Managers; however, you must ensure that proper security settings have been put into place before allowing self-registration.



The self-registration feature is turned off by default (for both fresh installs and upgrades); thus, you'll need to enable it under your *Security* configuration. Here, you can choose between *none* (not allowed), *moderated* (an administrator must approve the account before it is created), and *unmoderated* (once a user registers, his or her account will be automatically created). If you allow self-registration, the moderated setting is recommeded for security. Please review the *Security* configuration topic for additional information.

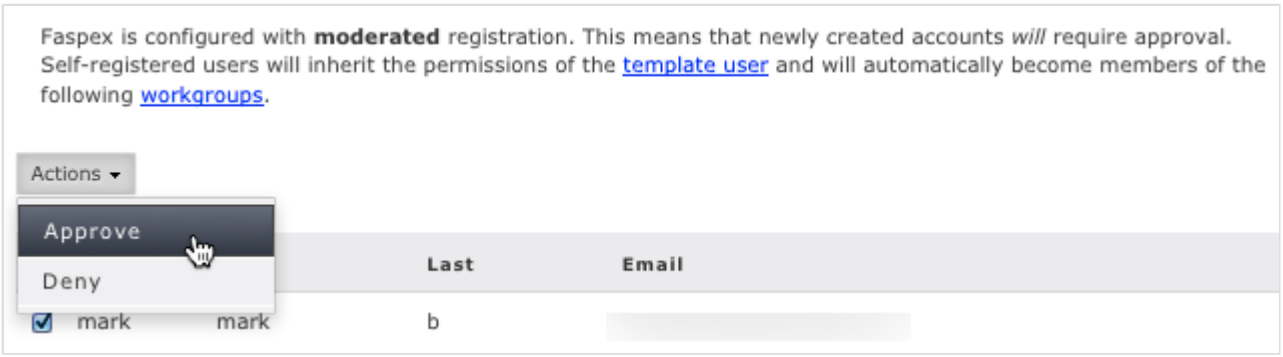


This topic assumes that you have turned on the *moderated* self-registration setting. Once a user self-registers, you will see the **Pending Registrations (X)** tab under your **Accounts** menu (where **X** stands for the number of pending registrations).



Approving or Denying a Pending Registration

To approve or deny a pending registration or group of pending registrations, mark the corresponding checkbox(es). Then, select either **Approve** or **Deny** from the **Actions** drop-down list.

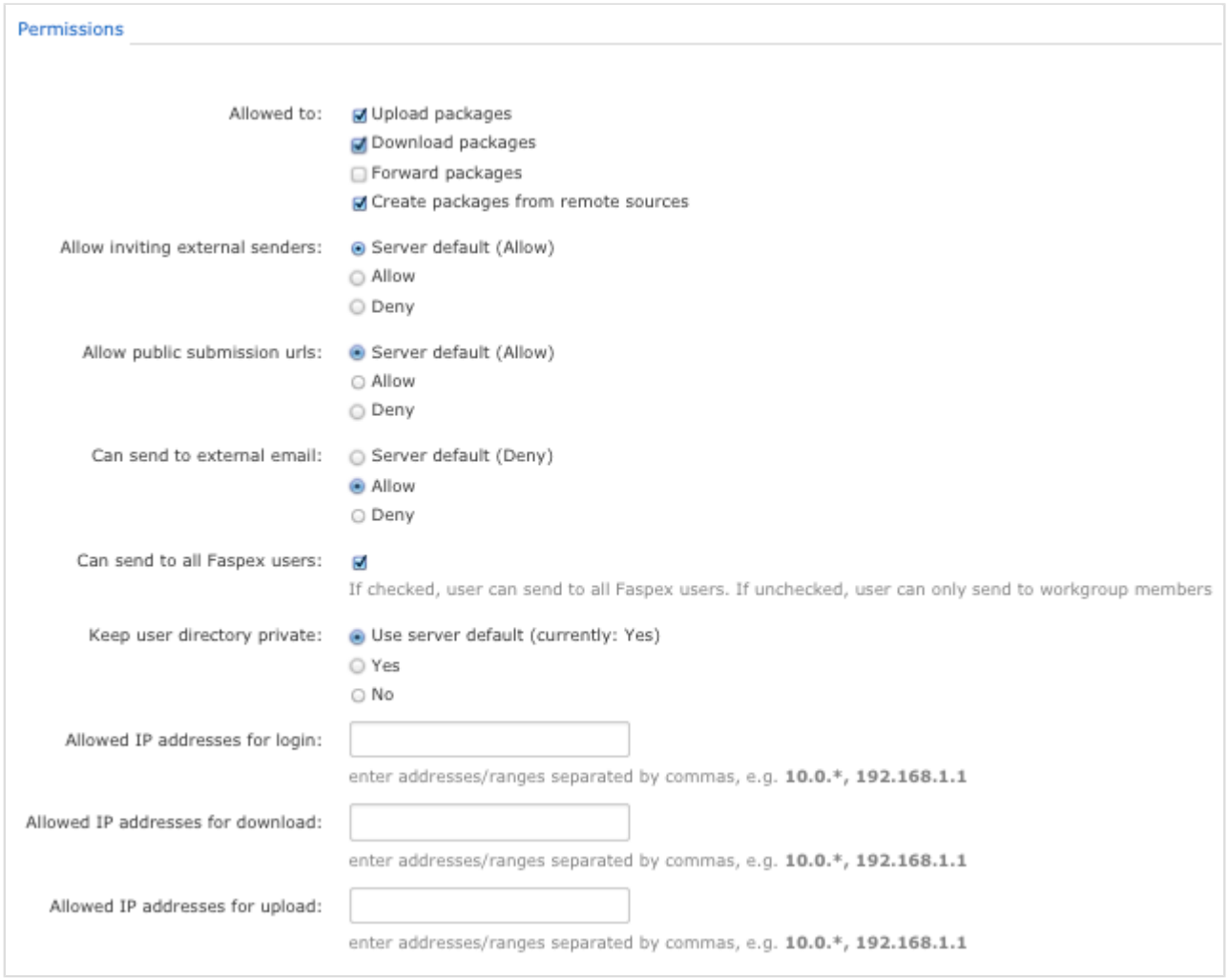


If you approve users, they will automatically inherit the permissions of the template user and will become members of a workgroup(s), if configured to do so. Note that you still update their permissions and workgroup memberships from the **Users** tab.

Changing Permissions for the Template User

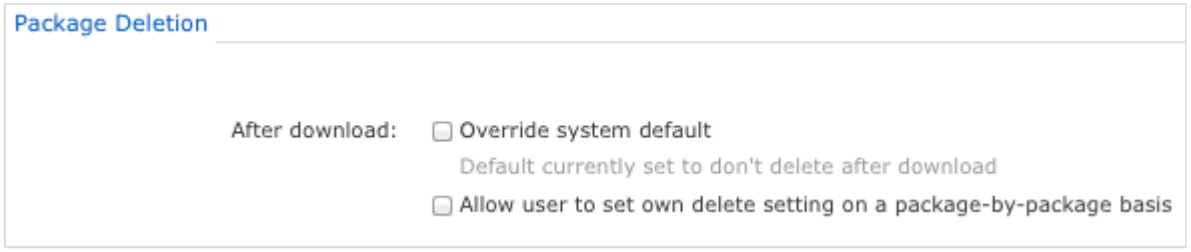
As described above, approved users will inherit the permissions of the template user. This user has default settings, which you can view and modify by clicking **template user** link. On the **Edit Template User** page, you will find the following settings:

Option	Description
Account expires	*(Disabled by default)* Enable this setting if you would like a self-registered user's account to expire (i.e. deactivate) after "X" number of days (where "X" is any integer). Once the account expires, that user will no longer be able to log into Faspex, unless you re-activate the account. Note that within the **Accounts** list, *inactive* accounts are shown in gray. Packages sent to this user will remain on the server (if configured to do so).
Account auto-deletes	*(Disabled by default)* Enable this setting if you would like a self-registered user's account to auto-delete after after "X" number of days (where "X" is any integer). Note that if this setting is enabled, the user's account will be completely removed from the Faspex database and you cannot re-activate it. Packages sent to this user will remain on the server (if configured to do so).



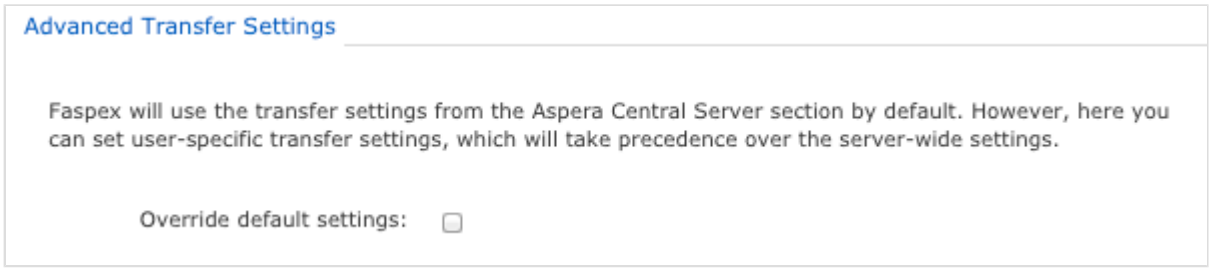
Option	Description
Upload Packages	Enable allowing the user to send file packages.
Download Packages	Enable to allow the user to download packages that have been received. A user who does not have this marked will still receive packages, but will not be able to download the files.
Forward Packages	Enable to allow the user to forward received file packages to other users. The package will be made accessible to the forwarded users within their Faspex accounts.
Create packages from remote sources	Enable to allow user to create a package from a remote source (i.e. a remote server, which is configured via the Aspera Node API). Note that this setting is ON, by default, and that it must be set on a per-user basis (i.e. there is no global option).
Allow inviting external senders	When enabled, external senders (those who do not have Faspex accounts) can be invited to send a package. Changing this user setting overrides the system default (set under *Security*).
Allow public submission URLs	A Public URL can be used by external senders to submit packages to registered Faspex users. The benefit of using a Public URL is in the time-savings, such that external senders no longer need to be individually invited to submit a package (although that functionality still exists). When a Public URL is enabled and posted to a an email, instant message, website, etc., the following workflow occurs: 1. **The external sender clicks the Public URL.** 2. **The sender is directed to page where he or she is asked to enter and submit an email address.** 3. **A private link is *automatically* emailed to the sender.** 4. **The sender clicks the private link and is automatically redirected to the Faspex-user package submission page.** 5. **Once the package is submitted through the private link, the Faspex user receives it.** Thus, when the field **Allow public submission URLs** is enabled (e.g. set to `Allow`), the Public URL feature is turned on for this user. If set to `Deny`, then the feature is turned off for this user. Note that changing the user setting overrides the system default (set under *Security*). **IMPORTANT NOTE:** Even if the Public URL feature is enabled for a registered Faspex user, he or she can override the feature for their own account by going to **Preferences** > **Misc** > **Enable public URL** and disabling the checkbox.
Can send to external email	Enable to allow the user to send a download link to external emails addresses (which are not Faspex users).

Option	Description
Can send to all Faspex users	Enable to allow the user to send packages to all Faspex users (as opposed to only being able to send packages to the user's workgroup members).
Keep user directory private	Override the default system setting to either allow users to see all other users, or prevent them from seeing all other users.
Allowed IP addresses for login	Specify the IP address(es) that a Faspex user can login from to view his or her account. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).
Allowed IP addresses for download	Specify the IP address(es) that a Faspex user can login from to download packages. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).
Allowed IP addresses for upload	Specify the IP address(es) that a Faspex user can login from to upload packages. A wildcard (*) can be used in this option (e.g., 192.168.10.*., which allows the user to login from 192.168.10.1, 192.168.10.2, etc.). Separate multiple email addresses with commas (,).



Options available **after downloading** a package:

Option	Description
Override system default	If you opt to override the system default, you can enable one of the following actions to occur after downloading: • Do nothing • Delete files after **any recipient** downloads all files • Delete files after **all recipient** download all files
Allow user to set own delete setting on a package-by-package basis	Provide the policy settings in the user's **New Package** screen. The user can determine the file package's expiration rule when preparing it.



Faspex uses the transfer settings from the Aspera Central Server section by default. However, when **Override default settings** is checked, you can set user-specific transfer settings, which will take precedence over the server-wide settings.

Option	Description
Initial Transfer Rate	Specify the initial upload and download transfer rate. When the option **Lock minimum rate and policy** is checked, the user will not be able to adjust transfer policy or minimum transfer rate.
Maximum Allowed Rate	Specify the initial upload and download transfer rate.

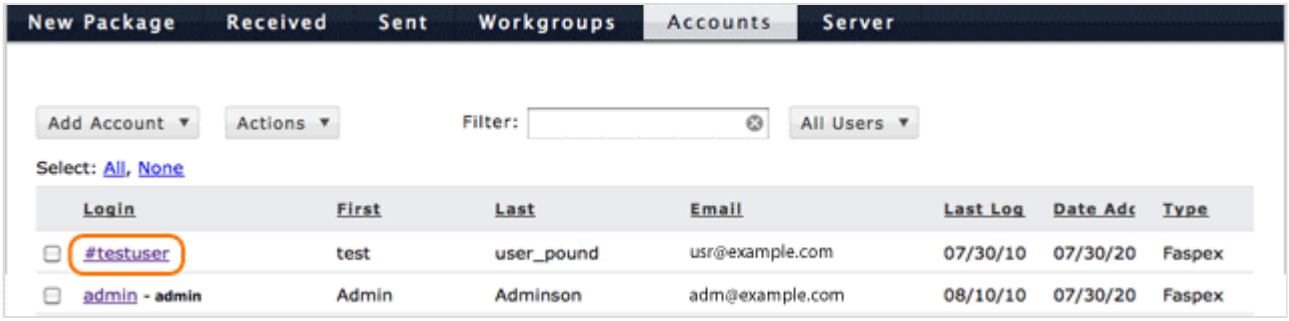
Managing Faspex Users

Manage and remove Faspex user accounts.

You can edit, manage and remove Faspex user accounts via the *Accounts* menu option. The following screenshots depict basic functionality:

Edit a Faspex Account

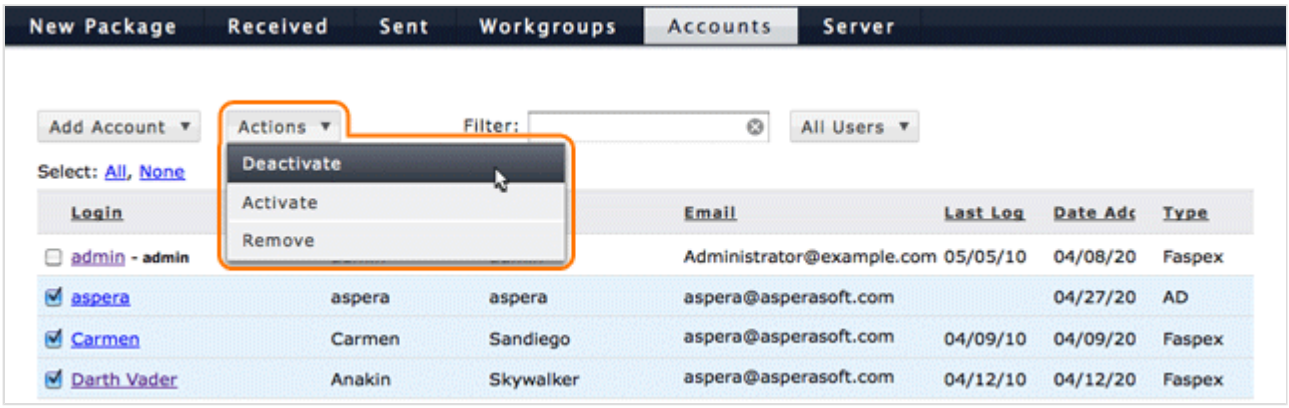
Once an account is created, you can later modify it by clicking the corresponding name link.



Activate or deactivate Faspex accounts

A Faspex user's account must be *activated* before he or she can log in to the server. To activate a user (or multiple users), check the corresponding box(es) and click **Actions** > **Activate** . Conversely, to deactivate users, select one

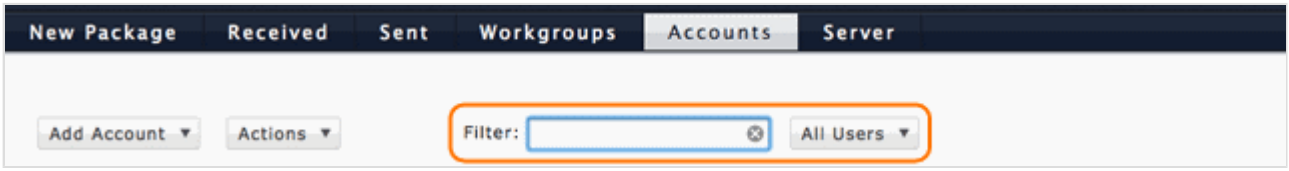
or several accounts on the user listing page and click **Actions** > **Deactivate** . Note that within the user account list, *inactive* accounts are shown in gray.



NOTE: You can change the number of rows displayed in the list through *Account (Preferences)* on page 29.

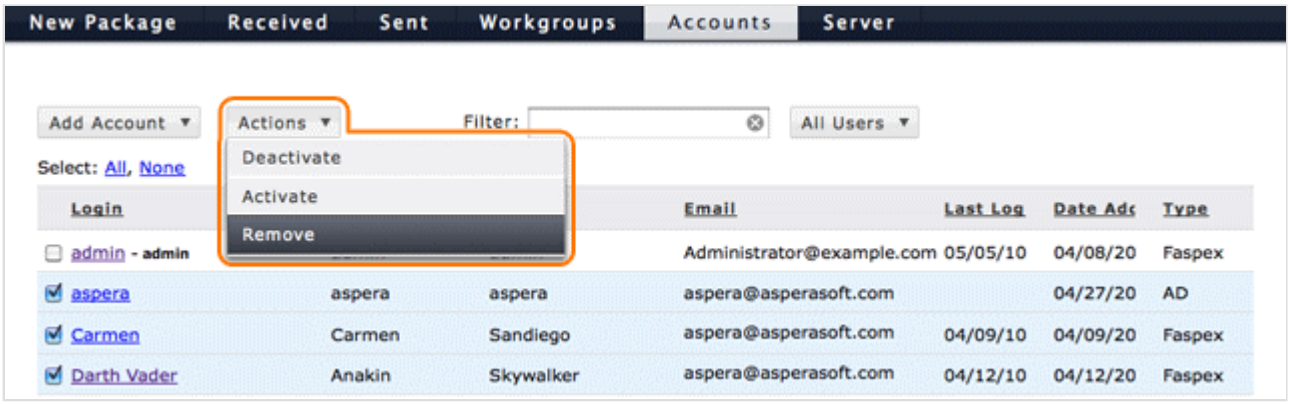
Sort or Filter accounts

To sort users, click a link in the header bar to sort them. For example, when clicking *Login*, all accounts are sorted alphabetically by login. Click again to sort in reverse order. You can use the filter controls to search for users or restrict display to users of a certain type. The filter searches through the following fields: **first name**, **last name**, **username**, **email**, and **description**. To search, enter keywords in the **Filter** field or select a user type from the drop menu.



Remove Faspex accounts

To remove users, select one or multiple users in user listing, and click **Actions** > **Remove**.



NOTE: When viewing a Faspex user's account, you click the **Workgroup Memberships** link to view a list of workgroups and/or dropboxes that they are currently associated. You may also add the user to workgroups and/or dropboxes from this link. For additional information on adding users to workgroups and/or dropboxes, please view the topic *Add Users to Dropboxes and Workgroups* on page 129.

Workgroup and Dropbox Management

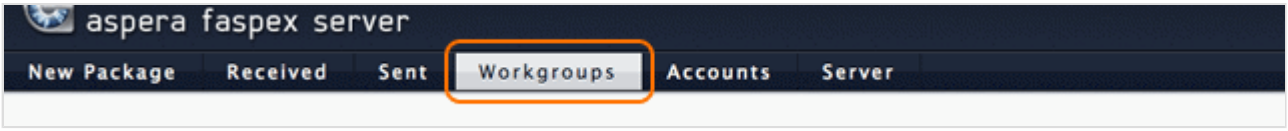
Create and manage Faspex workgroups and dropboxes

Create and Manage Workgroups

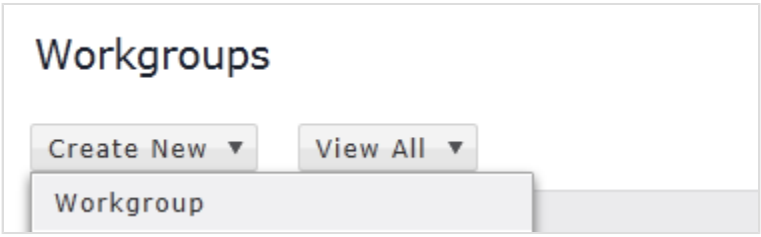
Administering the Faspex Workgroup feature

In Faspex, you can use workgroups to determine how the users in a group transfer files, and whom the user can send packages to. Workgroups can be set up by either a Faspex administrator or manager, however workgroup administrators cannot create workgroups, Workgroup administrators manage specific workgroups according to the permissions set in that workgroup for that role.

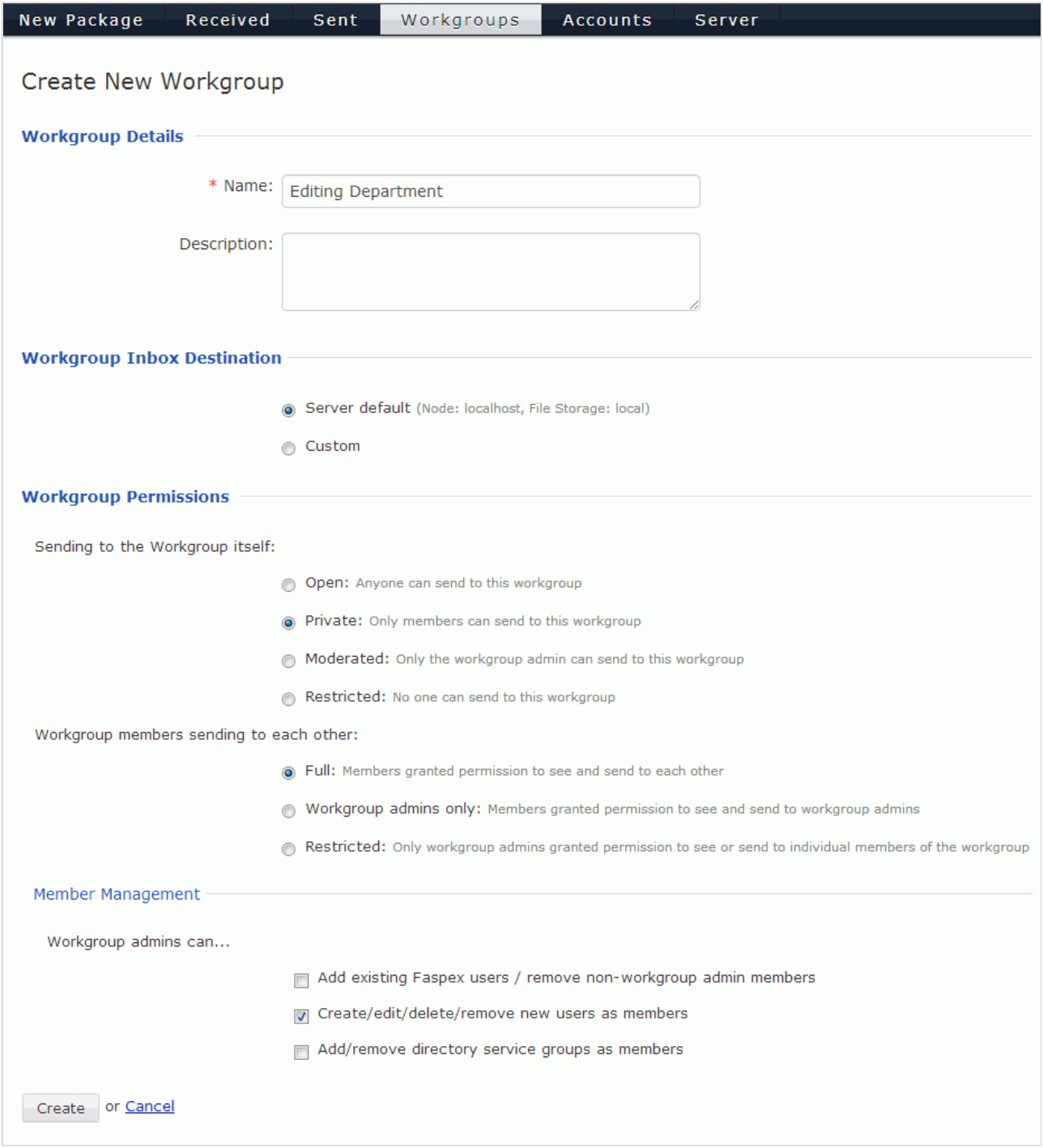
To set up a workgroup, select **Workgroups** from the Faspex menu.



Then go to **Create New** > **Workgroup**.



Enter the following information in the *Create New Workgroup* screen:



Workgroup Details

Option	Description
Name	The workgroup's name.
Description	The workgroup's description.

Workgroup Inbox Destination

Option	Description
Server Default	The UI label for **Server Default** displays the node and directory for the current default file storage that is serving as the inbox. (For a fresh installation, the default inbox node is **localhost** and file storage is **local**).
Custom	Opens a listing of file storage locations you can choose from to serve as a workgroup-specific inbox. NOTE 1: The location of a workgroup inbox can only be set by a Faspex administrator. It cannot be set by a workgroup administrator. NOTE 2: When a custom inbox is used, incoming packages will wind up in two locations: the custom location, and the server default location. When packages are deleted from the default location by means of the UI, they are not automatically removed from the custom location. NOTE 3: Packages are never deleted from a custom workgroup inbox if it is different from the default inbox. Settings for automatic deletion of packages after downloads or at expiration do not apply. NOTE 4: Even if symlinking is enabled for a storage location, packages sent to a workgroup or dropbox with a custom inbox will not be symlinks. The default inbox location will contain symlinks, but custom inboxes will contain actual files.

Workgroup Permissions: Sending to the Workgroup itself

Option	Description
Open	All Faspex users can upload packages to the this workgroup. Members of this workgroup can download files from it.
Private	Only members of this group can upload and download packages to/from this workgroup.
Moderated	Only the workgroup administrator(s) can send packages to this workgroup. Members of this workgroup can download files from it.
Restricted	No one can send to this workgroup. Members of this workgroup can download file packages from it.

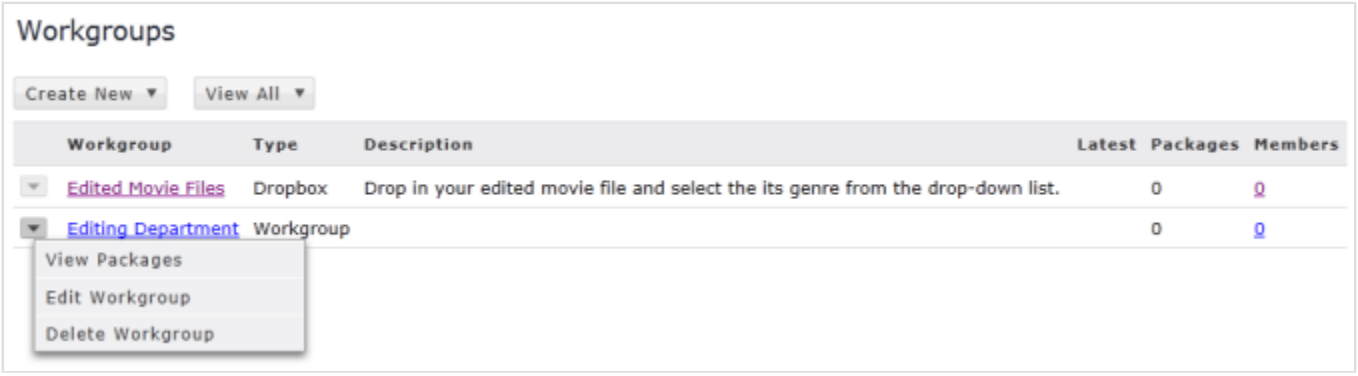
Workgroup Permissions: Workgroup members sending to each other

Option	Description
Full	Members of this workgroup can see and send packages to one other.
Workgroup admins only	Members of this workgroup can only see and send packages to workgroup admin(s).
Restricted	Members cannot see or send packages to anyone else in the workgroup; however, for Faspex Server versions 2.5.1+, workgroup *admins* can see and send packages to individual members in the workgroup.

Member Management: Workgroup admins can...

Option	Description
Add/remove existing users as members	The workgroup administrator can add or remove existing Faspex users to/from this workgroup.
Create/edit/delete new users as members	The workgroup administrator can create new Faspex users and add or remove them from this workgroup.
Add/remove directory service groups as members	The workgroup administrator can add or remove Directory Service groups from this workgroup.

When finished, click the **Create** button to continue. The view changes to the *Editing Workgroup* view, which includes a **Workgroup Members** section at the bottom of the display. Here you can add members and designate a workgroup administrator. Your new workgroup will be listed on the *Workgroups* page, along with any other dropboxes or workgroups that have been created. By clicking the corresponding down-arrow button, you can view the workgroup's packages, edit the workgroup, or delete it.



You can also click the number of members link on the right side of the table to add Faspex users to the workgroup. For additional details, see *Add Users to Dropboxes and Workgroups* on page 129.

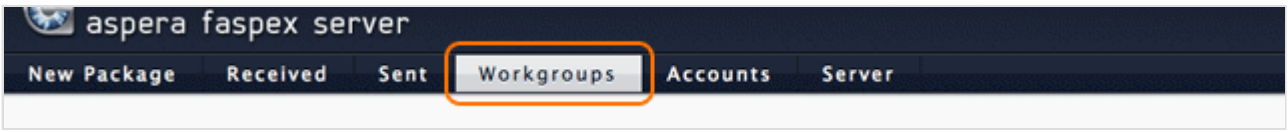
Create and Manage Dropboxes

Administering the Faspex Dropbox feature

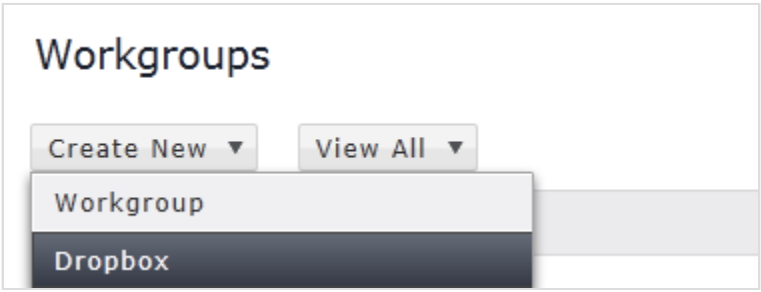
The Faspex Dropbox feature offers the following capabilities:

- Allows file submission for various projects and business processes, with the ability to specify different required metadata for each.
- Allows outside users to drop packages in file submission areas without having full access to the Faspex Server.

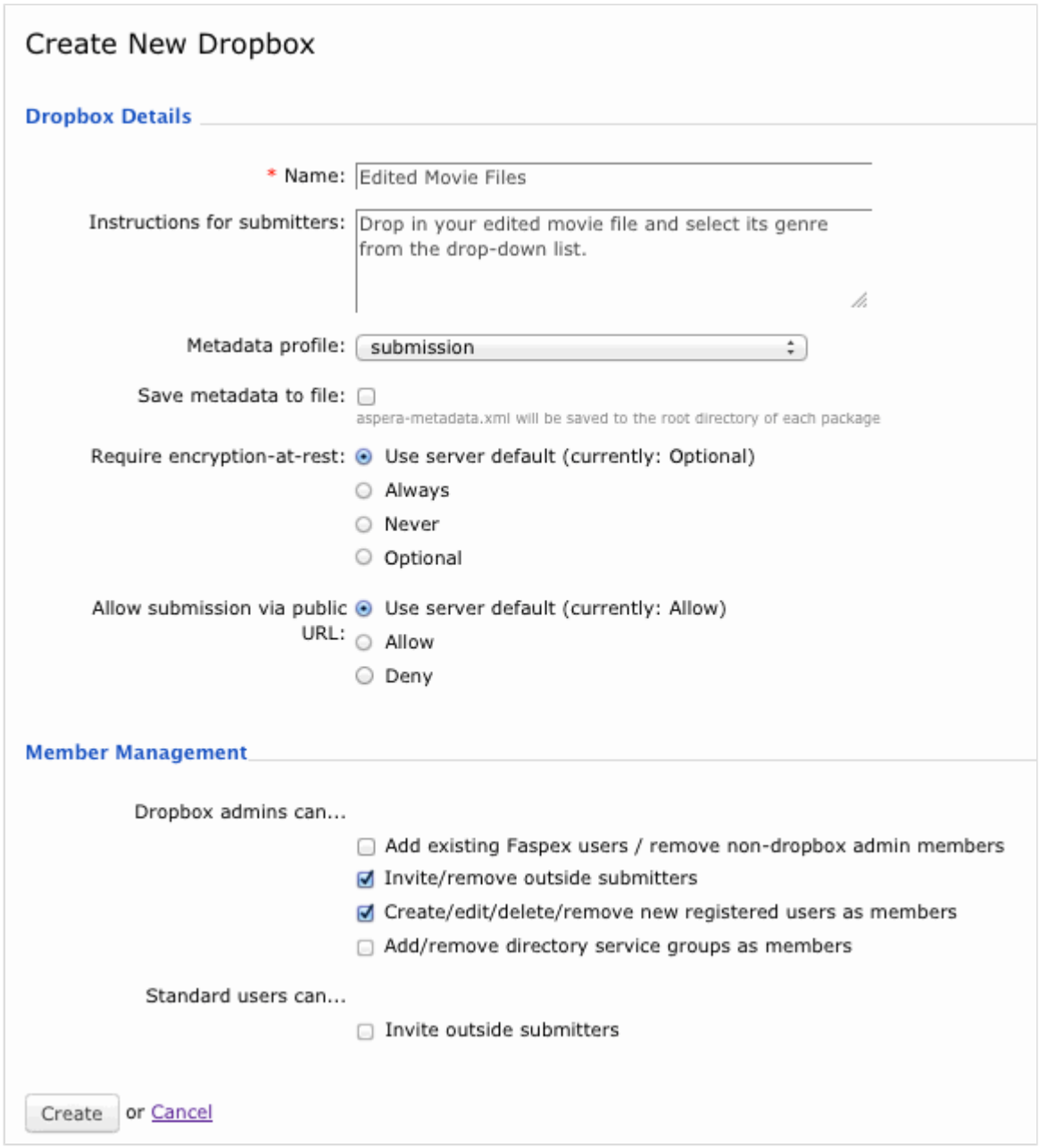
To set up a Faspex Dropbox, select **Workgroups** from the Faspex menu.



Then go to **Create New** > **Dropbox**.



Enter the following information within the *Create New Dropbox* screen:



Dropbox Details

Option	Description
Name	The dropbox's name.
Description	The dropbox's description.
Metadata profile	Select a metadata profile from the drop-down list or indicate none. Recall that metadata is additional information that a user can send with a file package. An Administrator can designate which metadata profile each dropbox's "Submit Package" page will use, based on metadata profiles that have been configured via **Server**

Option	Description
	> **Metadata**. Every dropbox that you create can have a unique metadata profile. For help on setting up your metadata profiles for dropboxes and normal package submissions, please view the topic *Metadata* on page 94
Save metadata to file	If enabled, a package's metadata is saved to its root directory (in the file `aspera-metadata.xml`). If **SaveMetadataInPackage** is also set to "true" in the configuration file `faspex.yml`, `aspera-metadata.xml` is instead inserted inside packages, and will be visible when the package contents are viewed in Faspex. For details about faspex.yml options, see *Advanced Config Options* on page 105.
(DEPENDS ON SECURITY CONFIGURATION) Require encryption-at-rest (EAR)	The following fields will appear if you have enabled the "Allow dropboxes to have their own encryption settings" checkbox within **Server** > **Configuration** > **Security** . Please see *Security* on page 56 for details. • **Use server default** • **Always:** Always use EAR. When enabled, users will be required on upload to enter a password to encrypt the files on the server. Subsequently, recipients will be required to enter the password to decrypt protected files as they are being downloaded. Note that if a user elects to keep downloaded files encrypted, then they do not need to enter a password until they attempt to decrypt the files locally. **This feature is not fully enforced unless the Faspex Server Administrator also updates the aspera.conf configuration file (which is not automatically modified by Faspex).** The Administrator may update *aspera.conf* manually, as well as using the Aspera Enterprise Server GUI. *For additional information, please refer to Note on Encryption at Rest on page 163.* • **Never:** Do not use EAR • **Optional:** User may choose at send time whether to encrypt or not
Allow submission via public URL	**IMPORTANT NOTE:** This field and radio buttons will not appear if **(1)** Public URLs are disabled server-wide or **(2)** changing Public URLs have been disabled for individual dropboxes. A Public URL can be used by external senders to submit packages to both registered Faspex users and dropboxes. The benefit of using a Public URL is in the time-savings, such that external senders no longer need to be individually invited to submit a package (although that functionality still exists). When a Public URL is enabled and posted to a an email, instant message, website, etc., the following workflow occurs: 1. **The external sender clicks the Public URL for the dropbox.** 2. **The sender is directed to page where he or she is asked to enter and submit an email address.** 3. **A private link is *automatically* emailed to the sender.**

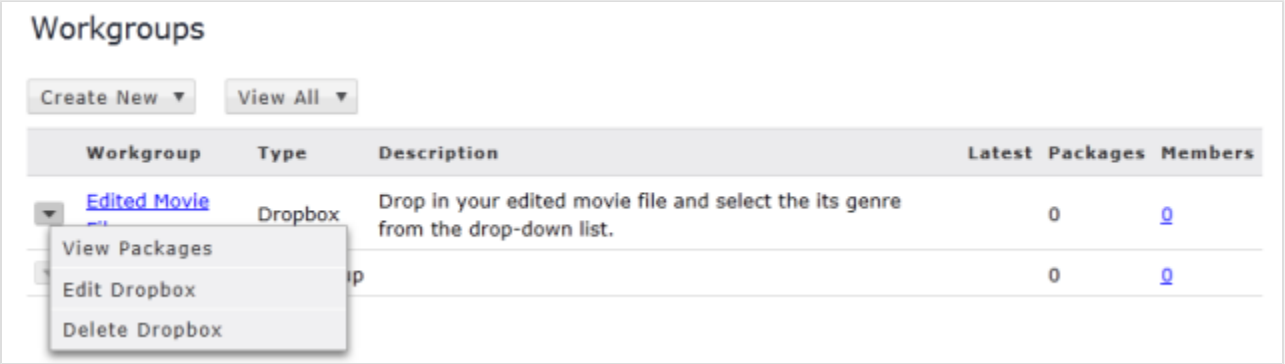
Option	Description
	4. **The sender clicks the private link and is automatically redirected to the dropbox package submission page.** 5. **Once the package is submitted through the private link, the dropbox receives it.** Thus, when the field **Allow submission via public URL** is enabled (e.g. set to `Allow`), the Public URL feature is turned on for this dropbox. If set to `Deny`, then the feature is turned off for this dropbox. Note that changing the dropbox setting overrides the system default (set under *Security*).

Member Management

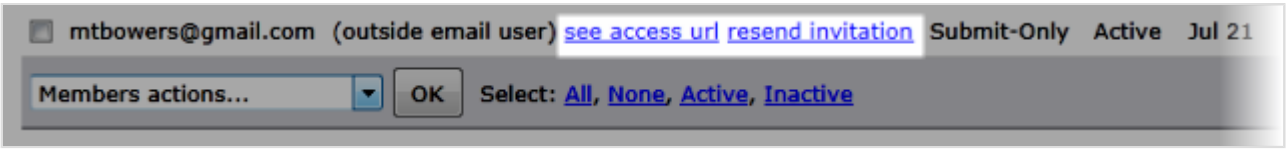
Option	Description
Dropbox admins can...	• Add/remove existing users as members • Invite outside submitters • Create/edit/delete new registered users as members • Add/remove directory service groups as members
Standard users can...	Invite outside submitters

WARNING: When outside submitters are invited to access a dropbox, they are not prevented from sharing the upload link with others. Aspera records the IP address used to submit packages; however, Faspex Server cannot verify that the person who is using the link is actually the intended invitee. If this is a concern to your organization, then you can identify one of two security options when sending an invitation to an outside submitter: the submission link expires **after one successful upload COMPLETION** or the submission link expires **on a specific date**. Note that for the case of expiration after the completion of a successful upload, it *is* possible for an outside submitter to initiate parallel uploads using a single link; thereby submitting multiple packages. Please refer to the topic *Add Users to Dropboxes and Workgroups* on page 129 for additional details on setting up outside submitter security options.

When finished, click the **Create** button to continue. Your new dropbox will be listed on the *Workgroups* page, along with any other dropboxes or workgroups that you have created. By clicking the corresponding **down arrow** button, you can view the dropbox's packages, or edit and delete the dropbox, itself. You may also click the number of members link on the right side of the table to add Faspex users to the dropbox. For additional details on adding members, please go to the topic *Add Users to Dropboxes and Workgroups* on page 129.



NOTE ON INVITING OUTSIDE SUBMITTERS: After inviting an outside submitter, you can view the upload access URL, as well as resend the invitation. To do so, select the **Workgroups** tab in the Faspex menu, then click the **down arrow** button next to the corresponding dropbox. Select **Edit Dropbox** from the list. Then, on the *Editing Dropbox* page, scroll down to the **see access URL** and **resend invitation** links in the invited user's row.



Add Users to Dropboxes and Workgroups

Add Faspex users (members) to your Dropboxes and Workgroups

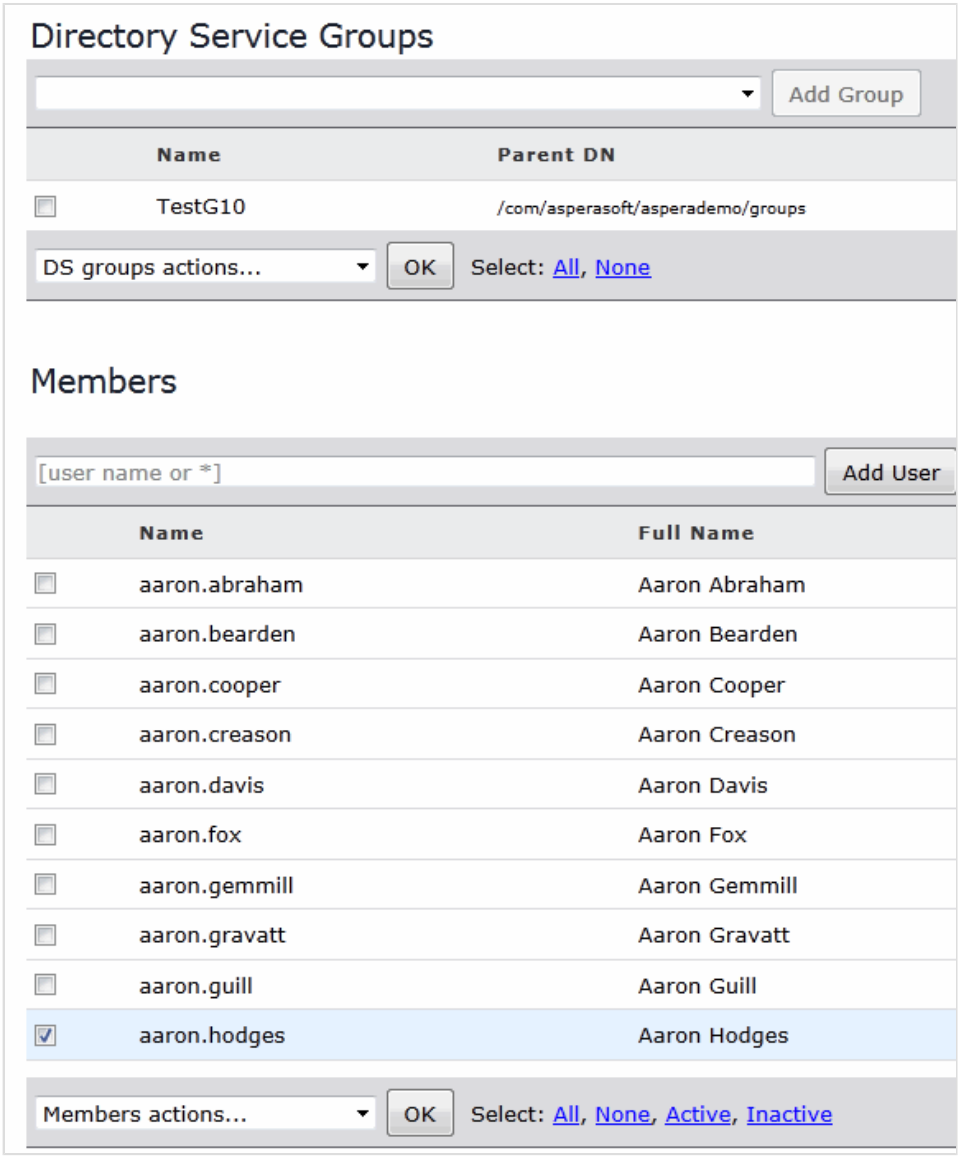
Workgroups and Dropboxes are listed under **Workgroups**, along with the number of associated members (see link on right side of table). To add/remove members to a dropbox or workgroup, as well as to add members via a Directory Service (DS) group that you have imported into Faspex, click the *Members* link for the dropbox/workgroup.

Adding a Directory Service (DS) Group to a Workgroup or Dropbox

IMPORTANT NOTE: You must first import the DS Group into Faspex by following the instructions in the topic *Authentication: Directory Service* on page 77.

1. **If a DS Group is available, it will appear in the Directory Service Groups drop-down list. Select the DS Group that you want to add to the workgroup or dropbox and click the Add Group button.**
2. **Once the group is added, it will appear in the directory service groups list. In addition, members of the added DS Group will automatically appear under the members list.**

3. **For dropboxes, you can manage DS group options by clicking the DS groups actions... drop-down list. Select from any one of the following options: Set standard access, Set submit-only access and Remove.**
4. **For dropboxes and workgroups, you can manage DS member options by checkmarking the appropriate member(s) and clicking the Members actions... drop-down list. For details on available actions, please refer to *Step 3* in the appropriate section below.**



Adding/Editing Workgroup Members (Faspex User Accounts and DS User Accounts)

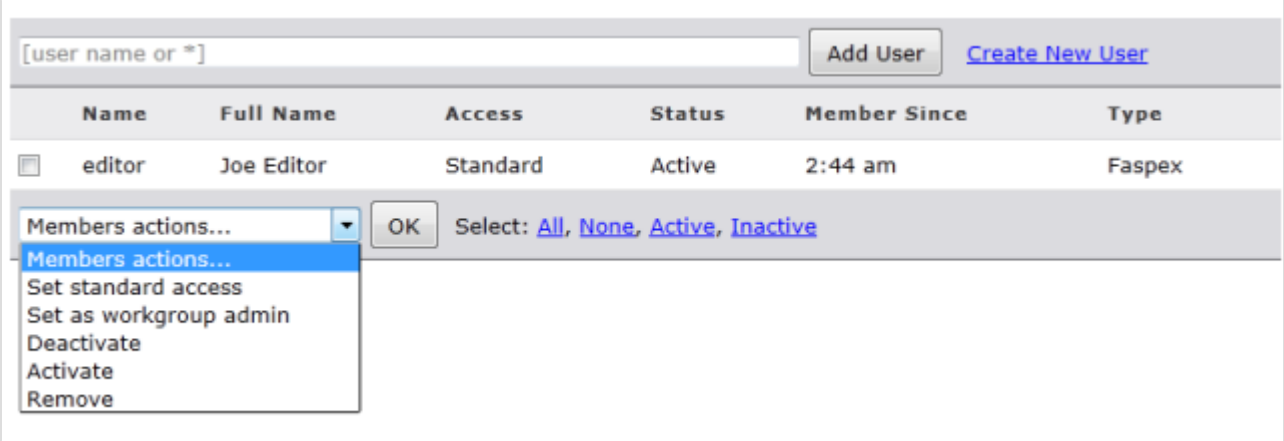
1. **Type in the user's name and click the Add User button. If you want to create a new user to add to the workgroup, click the Create new user link. For more information on creating new users, please see the topic *Creating a New Faspex User* on page 108. Note that if your Faspex server has Directory Services configured and you have imported one or more DS groups, then you can also add the DS users or groups.**

For more information about configuring DS, please refer to the topic *Authentication: Directory Service* on page 77.

2. **Once the account(s) are added, they will appear in the workgroup membership list.**
3. **You can manage workgroup members by checkmarking the appropriate member(s) and clicking the Members actions... drop-down list. Select from any one of the following options: Set standard access, Set as workgroup admin, Deactivate, Activate and Remove. A deactivated member cannot perform workgroup functions; however, the account will remain in the workgroup list. A removed member will be deleted from the workgroup list, but will remain a Faspex user.**

Workgroup Administrator Role: A user that is designated a "workgroup administrator" (by a Faspex administrator or manager). Workgroup administrators manage specific workgroups according to the permissions set for that role in that workgroup. As long as a Faspex administrator or manager has allowed it, workgroup administrators can add or remove workgroup members, and they can create new regular users.

Workgroup administrators cannot set a custom workgroup inbox; that can only be done by a Faspex administrator or manager. Workgroup administrators cannot delete workgroup packages; however, they can archive them.

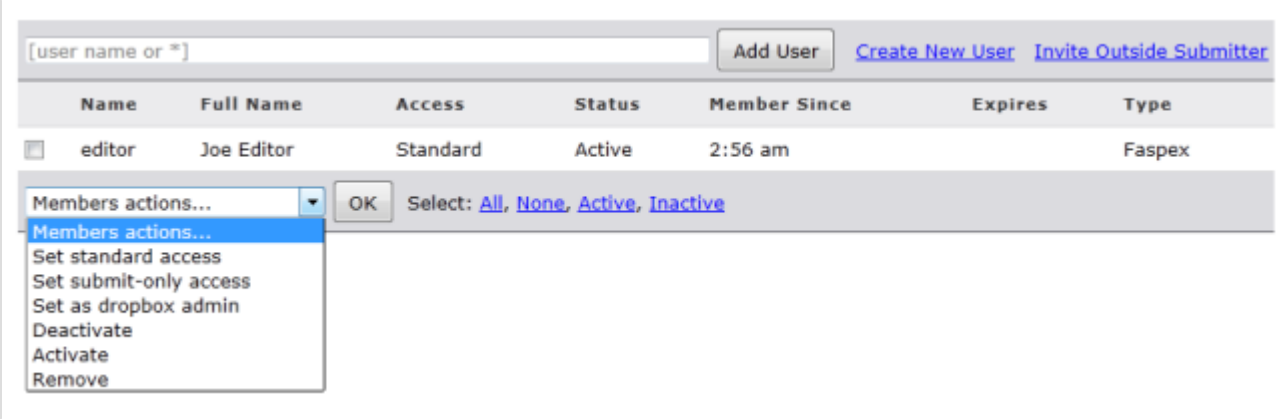


Adding/Editing Dropbox Members (Faspex User Accounts and DS User Accounts)

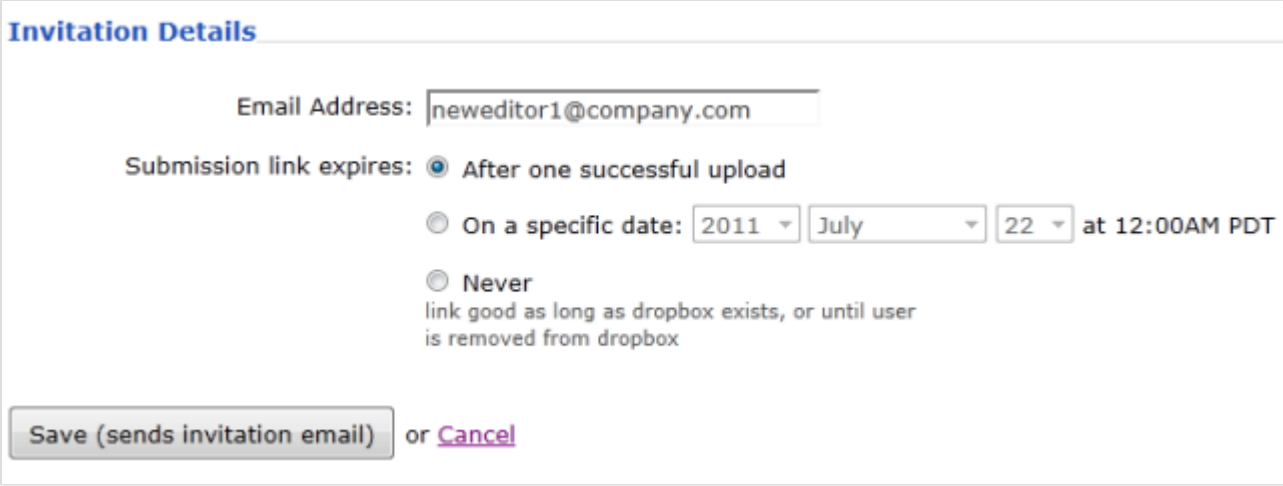
1. **Type in the user's name and click the Add User button. If you want to create a new user to add to the dropbox, click the Create new user link. For more information on creating new users, please see the topic *Creating a New Faspex User* on page 108. Note that if your Faspex server has Directory Services configured and you have imported one or more DS groups, then you can also add the DS users or groups. For more information about configuring DS, please refer to the topic *Authentication: Directory Service* on page 77.**
2. **Once the account(s) are added, they will appear in the dropbox membership list. For information on adding outside submitters, please see below.**

3. **You can manage dropbox members by checkmarking the appropriate member(s) and clicking the Members actions... drop-down list. Select from any one of the following options: Set standard access, Set submit-only access, Set as dropbox admin, Deactivate, Activate, and Remove. A deactivated member cannot perform dropbox functions; however, the account will remain in the dropbox list. A removed member will be deleted from the dropbox list, but will remain a Faspex user.**

IMPORTANT NOTE: A dropbox administrator can create regular users, and add or remove other members to/from the dropbox. Standard access includes uploading and downloading packages to/from the dropbox. Submit-only access limits users to only being able to submit to the dropbox, without being able to download.



If your dropbox configuration allows it, you can also click the **Invite Outside Submitter** link to send an invitation to a non-Faspex user.



You must complete the following fields to invite an outside submitter to the dropbox:

Field	Description
Email Address	The outside submitter's email address (this is where the invitation will be sent).
Submission link expires	• **After one successful upload:** The outside submitter can only submit one package. • **On a specific date:** The outside submitter has until the date selected to submit to the dropbox. • **Never:** The link will work as long as the dropbox exists, or until the outside submitter is removed from the dropbox. **WARNING:** When outside submitters are invited to access a dropbox, they are not prevented from sharing the upload link with others. Aspera records the IP address used to submit packages; however, Faspex Server cannot verify that the person who is using the link is actually the intended invitee. If this is a concern to your organization, then you can identify one of two security options when sending an invitation to an outside submitter: the submission link expires **after one successful upload COMPLETION** or the submission link expires **on a specific date**. Note that for the case of expiration after the completion of a successful upload, it *is* possible for an outside submitter to initiate parallel uploads using a single link; thereby submitting multiple packages.

Click **Save (sends invitation email)** to complete this process. For information on customizing your invitation email templates, please refer to the topic *Notifications* on page 68.

Maintaining Faspex

Basic Faspex management, such as restarting services, changing admin password, and configuring the web server.

Bandwidth Measurement

Enable bandwidth discovery feature that measures bandwidth prior to uploads.

You can enable bandwidth measurement that causes all uploads to perform a bandwidth measurement prior to transferring regardless of the target rate setting for the server or the transferring user (downloads are not affected). Follow these steps to configure:

1. Stop Faspex

   In a Terminal or Command Prompt, execute the command to stop Faspex:

   ```
   asctl faspex:stop
   ```

2. Add bandwidth measurement parameter in *Faspex.yml*

   Locate *Faspex.yml* in the following path:

OS Version	Path
32-bit Windows	C:\Program Files\Aspera\Faspex\config\Faspex.yml
64-bit Windows	C:\Program Files (x86)\Aspera\Faspex\config\Faspex.yml

   Before editing *Faspex.yml*, create a backup. Open it with a text editor, and add this line at the end of the file:

   ```
   ...
   MeasureBandwidthOnUpload: yes
   ```

3. Start Faspex

   In a Terminal or Command Prompt, execute the command to start Faspex with the new setting:

   ```
   asctl faspex:start
   ```

To verify bandwidth measurement, open Aspera Connect and go to **Preferences** > **Bandwidth**, click **Remove All** and make sure **Automatically cache measurements obtained during transfer** is unchecked. Now log into Faspex and send a package. In the first few seconds of the transfer, Connect should show a status of *Measuring Bandwidth...*.

Changing Package Directory

Change Faspex Server's package storage directory.

You may utilize an *asctl* command to change the Faspex Server package storage directory. To view the current package directory, run the following command in a *Command Prompt* window:

```
> asctl faspex:package_dir
```

To *change* Faspex Server's package directory, use the same command, but specify a path *(e.g., change to C:\new-path)*:

```
> asctl faspex:package_dir C:\new-path
```

IMPORTANT NOTE: *Changing the package directory within the application does not move the packages or create the directory.* The Faspex Server Administrator must create the new package directory and move the packages manually on the file system, being careful to preserve the directory permissions. Copying packages can be performed either *before* or *after* changing the package directory. For additional assistance, please contact *Technical Support* on page 175.

SPECIAL CONSIDERATIONS:

If you will be storing Faspex packages in a network directory, ensure that the directory is configured as follows:

- The network share is accessible to the OS system account that Faspex Server is running under, with permissions to read/write/delete/traverse directories, and create new files and folders.
- UNC paths are used, rather than drive letters.
- If you are using Active Directory (AD) and the network share uses AD to manage permissions, check that Faspex Server and Aspera Central are running under a domain account.

Modify HTTP Server Settings

Configure the Apache HTTP Server used by Faspex.

You may configure Faspex's Apache HTTP Server to use different host name, communication port, and namespace.

IMPORTANT NOTE: For help on regenerating the self-signed SSL certificate (due to a host name change) that is installed with this Aspera Web application, please refer to the topic *> Regenerate Self-Signed SSL Certificate (Apache)* on page 43. For instructions on creating and enabling a CA-signed certificate, please refer to the topics *> Create an SSL Certificate (Apache)* on page 39 and *> Enable SSL (Apache)* on page 42, respectively.

To begin, in a Command Prompt (**Start menu** > **All Programs** > **Accessories** > **Command Prompt**), execute the following command to navigate into the Faspex directory:

OS Version	Command
32-bit Windows	`> cd "C:\Program Files\Aspera\Faspex"`
64-bit Windows	`> cd "C:\Program Files (x86)\Aspera\Faspex"`

1. Update the hostname

   The hostname used by apache is configured when you first install Faspex. Use this command to print the current hostname:

   ```
   > asctl apache:hostname
   ```

   To change the hostname, use the following command. Replace **HOSTNAME** with the new hostname:

   ```
   > asctl apache:hostname HOSTNAME
   ```

   Also update your SSL certificate to reflect the new hostname:

   ```
   > asctl apache:make_ssl_cert HOSTNAME
   ```

2. Change HTTP and HTTPS ports

   By default, Faspex uses standard ports for HTTP (80) and HTTPS (443). Use the following commands to update these ports:

Item	Command
HTTP	`> asctl apache:http_port NEW_HTTP_PORT`
HTTPS	`> asctl apache:https_port NEW_HTTPS_PORT`

3. Change Faspex namespace

   Faspex uses the namespace */aspera/faspex* by default. Use this command to print the current namespace:

   ```
   > asctl faspex:uri_namespace
   ```

   To set the namespace to, for example, **/faspex**, use the following command:

   ```
   > asctl faspex:uri_namespace /faspex
   ```

When the namespace is updated, advise your users of the new url. For example, if your faspex server's address is *10.0.0.10* and you change the namespace to "*/faspex*", they would use the following URL:

```
https://10.0.0.10/faspex
```

Refer to *asctl Command Reference* on page 165 for a complete asctl command reference.

Customizing New-User-Account Form

Make certain fields in the Add New User form mandatory.

You can customize the *New User Account* form by marking certain fields required (**Accounts** > **Add Account**). For example, if you marked the option **Password expires** required, that field becomes required when creating a user.

1. Stop Faspex

   In a Terminal or Command Prompt, execute the command to stop Faspex:

   ```
   asctl faspex:stop
   ```

2. Open *Faspex.yml* with a text editor

   Locate *Faspex.yml* in the following path:

OS Version	Path
32-bit Windows	C:\Program Files\Aspera\Faspex\config\Faspex.yml
64-bit Windows	C:\Program Files (x86)\Aspera\Faspex\config\Faspex.yml

   Before editing *Faspex.yml*, create a backup. Open it with a text editor:

3. Add required-field parameters

   The following fields can be marked as required:

   - Password expires: ...
   - Account expires: ...
   - Allowed IP addresses for login
   - Allowed IP addresses for download
   - Allowed IP addresses for upload

   Add the following parameters in the file. When a required field is specified, the option is checked and greyed-out; When a required field with default value is specified, a default value is presented in the option:

Parameter	Description
RequireUserPasswordExpires: yes	Make "Password expires" required. A value is required.
RequireUserAccountExpires: yes	Make "Account expires" required. A value is required.
RequireUserDescription: yes	Make "description" required.
RequireUserDescriptionWithDefault: "Default_value"	Make "description" required, and insert default value.
RequireUserAllowedIpAddressesForLogin: yes	Make "Allowed IP addresses for login" required.
RequireUserAllowedIpAddressesForLoginWithDefault: "Default_value"	Make "Allowed IP addresses for login" required, and insert default value.
RequireUserAllowedIpAddressesForDownload: yes	Make "Allowed IP addresses for download" required.
RequireUserAllowedIpAddressesForDownloadWithDefau "Default_value"	Make "Allowed IP addresses for download" required, and insert default value.
RequireUserAllowedIpAddressesForUpload: yes	Make "Allowed IP addresses for upload" required.
RequireUserAllowedIpAddressesForUploadWithDefault: "Default_value"	Make "Allowed IP addresses for upload" required, and insert default value.

For example, to make "Account expires" required, and "Allowed IP addresses for download" required with default value "10.0.*", add the following lines in *Faspex.yml*:

```
...
RequireUserAccountExpires: yes
RequireUserAllowedIpAddressesForDownloadWithDefault: "10.0.*"
```

4. Start Faspex

   In a Terminal or Command Prompt, execute the command to start Faspex with the new setting:

```
asctl faspex:start
```

When making fields required, log in Faspex with admin account and go to **Accounts** > **Add Account** > **Faspex User**. Red asterisks should appear near the fields that have been marked as required. Creating a user without specifying values for these fields should result in an error message to that effect.

Configuring HTTP and HTTPS Fallback

Configure HTTP/HTTPS Fallback via the Connect Server GUI or aspera.conf.

HTTP Fallback serves as a secondary transfer method when the Internet connectivity required for Aspera accelerated transfers (i.e., UDP port 33001, by default) is unavailable. When HTTP Fallback is enabled and UDP connectivity is lost or cannot be established, the transfer will continue over the HTTP protocol. The instructions below walk through

the process of setting up HTTP/HTTPS fallback. For additional information on configuring different modes and testing, please refer to the Aspera KB Article "*HTTP fallback configuration, testing and troubleshooting*."

NOTE ON FASPEX CONFIGURATION: Faspex Server requires HTTP Fallback configuration in both the Faspex Server Web GUI and Enterprise/Connect Server. For the case when the Faspex Web server and transfer server are on the same machine, Administrators typically do not need to modify their Enterprise/Connect Server settings, since running the command `asctl faspex:setup` configures them automatically. However, for the case when the Faspex Web server and transfer server are on different machines, Administrators must configure the transfer server and firewall ports in **ONE** of the following ways:

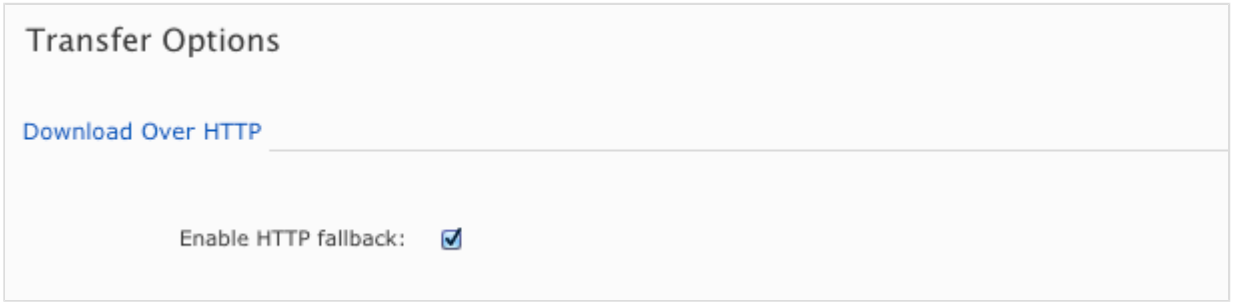
- HTTP/HTTPS enabled and set to defaults (8080 + 8443) *AND* firewall port open on 8080/8443.
- HTTP/HTTPS enabled and set to standard ports (80 + 443) *AND* firewall port open on 80/443.

Additionally, the transfer server's fallback settings must match Faspex's fallback settings; otherwise, Faspex will return a "Package creation failed" error. This includes ensuring that the transfer server has HTTP/HTTPS fallback enabled; and that (within the Web GUI) Faspex has **Server** > **Transfer Options** > **Enable HTTP Fallback** and **Server** > **Security** > **Encrypt Transfers** (for HTTPS fallback) turned on. For security, Aspera highly recommends using HTTPS fallback. If HTTPS fallback is enabled on the transfer server, then encrypted transfers must be enabled in the Faspex Web GUI.

NOTE ON ENCRYPTION-AT-REST: When a transfer falls back to the HTTP protocol, **Encryption-at-Rest** is no longer supported. If fallback occurs while *downloading*, then--despite entering a passphrase--the files will remain encrypted (i.e., enveloped). If HTTP Fallback occurs while *uploading*, then--despite entering a passphrase--the files will NOT be encrypted (i.e., enveloped).

1. *(Within Faspex Server administrative interface)* Turn on HTTP Fallback.

   Log into your Faspex Server's administrative interface and navigate to **Server** > **Configuration** > **Transfer Options** . Check **Enable HTTP Fallback**.



2. Confirm your HTTP Fallback port number.

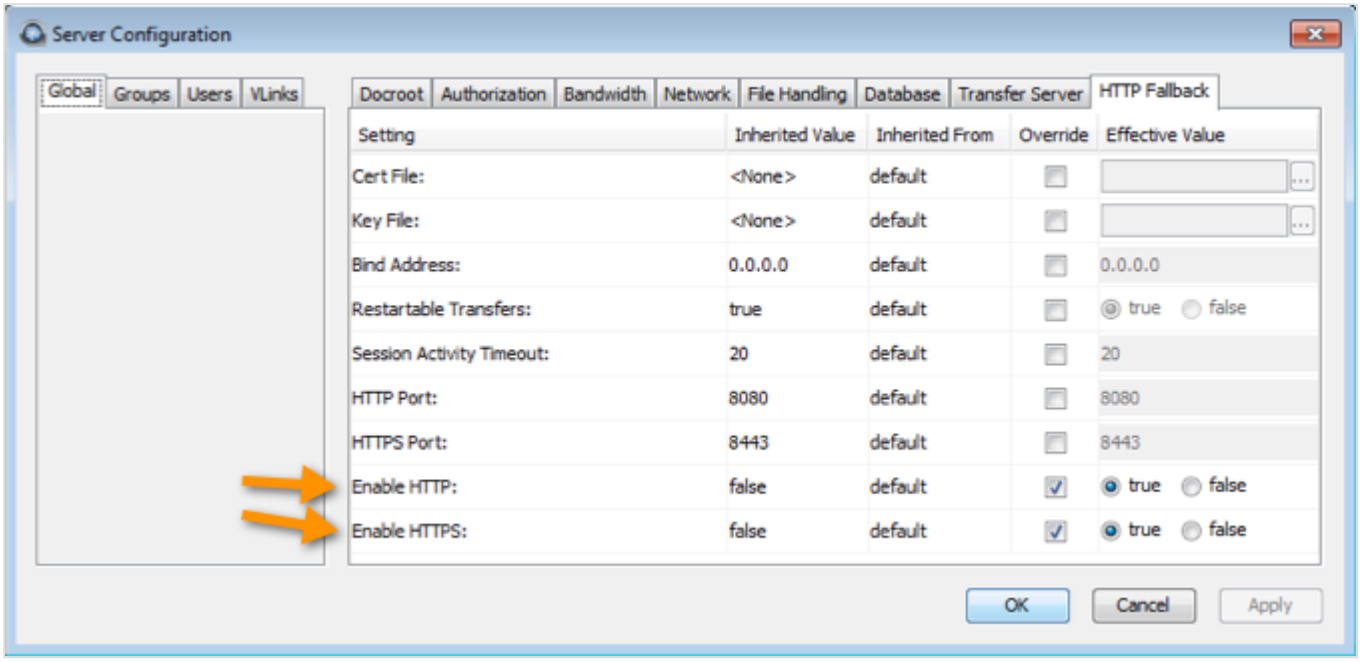
To confirm your HTTP Fallback port number, run the following `asctl` command in a *Command Prompt* window:

```
> asctl faspex:http_fallback_port
```

3. *(Within the Connect Server GUI)* Configure HTTP/HTTPS Fallback settings.

   To edit your settings, launch Connect Server and go to **Configuration** > **Global (tab in left pane)** > **HTTP Fallback (tab in right pane)** .

   - Set `Enable HTTP` to **true**.
   - If you want to allow fallback over HTTPS, set `Enable HTTPS` to **true**.



What do you do if you need to change your HTTP Fallback port number?

In the event that you need to modify your HTTP Fallback port number, please use the following `asctl` command (replacing `<port>` with your new port number):

```
> asctl faspex:http_fallback_port <port>
```

IMPORTANT NOTE: Do not use this command if the Faspex Web application and your transfer server are on the same machine. If you modify the HTTP fallback port for this particular setup, HTTP fallback will fail because Apache is hard-coded to route traffic to `asperahttpd` on port 8080.

Log Files

Faspex server's log files.

You will find log files for Faspex server and its associated components in the following directories:

OS Version	Path
32-bit Windows	• **Faspex**: C:\Program Files\Aspera\Faspex\log\ • **asctl**: C:\Program Files\Common Files\Aspera\Common\asctl\ • **MySQL**: C:\Program Files\Common Files\Aspera\Common\mysql\data\mysqld.log • **Apache**: C:\Program Files\Common Files\Aspera\Common\apache\logs\
64-bit Windows	• **Faspex**: C:\Program Files (x86)\Aspera\Faspex\log\ • **asctl**: C:\Program Files (x86)\Common Files\Aspera\Common\asctl\ • **MySQL**: C:\Program Files (x86)\Common Files\Aspera\Common\mysql\data\mysqld.log • **Apache**: C:\Program Files (x86)\Common Files\Aspera\Common\apache\logs\

In Faspex's Apache log folder, you will find the following files:

- access_log
- error_log
- ssl_access_log
- ssl_error_log
- ssl_request_log

IMPORTANT NOTE: Apache's log files are not automatically deleted. If you would like to remove old logs, it is recommended that you create a *windows scheduler job* to do so.

To further configure Faspex's Apache's log settings, execute the following commands in a command prompt (**Start** > **All Programs** > **Accessories** > **Command Prompt**):

Setting	Command
Specify Apache log level (e.g. error level)	`> asctl apache:log_level error`
Enable Apache log (i.e. set to notice)	`> asctl apache:enable_logs`
Disable Apache log (i.e. set to emerg level)	`> asctl apache:disable_logs`

Transfer logs are stored in the following location:

OS Version	Path
32-bit Windows	C:\Program Files\Aspera\Enterprise Server\var\log
64-bit Windows	C:\Program Files (x86)\Aspera\Enterprise Server\var\log

You will find the following component-based log files within the logs folder:

File Name	Description
ascmd.log	File browsing and manipulation in user interface.
asconfigurator.log	Server configuration information.
asperacentral.log	A server-side service that handles transfers, web services and database logging.
aspera-scp-transfer.log	The *fasp* transfers.
aspera-scp-http-transfer.log	The HTTP Fallback server.
asperasync.log	The Hot Folders (File synchronization).

IMPORTANT NOTE: Older log files are saved as the same file name, with an incremental number attached (e.g. ascmd.0.log).

Resetting Faspex Admin Password

Reset your Faspex's administrator password.

To reset Faspex's administrator password, execute the following command in a Command Prompt (**Start** > **All Programs** > **Accessories** > **Command Prompt**). Replace <name> with your existing admin login, <email> with admin email. Enter the account's password when prompted.

```
> asctl faspex:admin_user <name> <email>
```

You can also enter the admin's new password in the command:

```
> asctl faspex:admin_user <name> <email> <password>
```

Restarting Faspex

Restart Faspex if it is not working properly or to apply new settings.

To restart Faspex, execute the following command in a Command Prompt (**Start** > **All Programs** > **Accessories** > **Command Prompt**):

```
> asctl faspex:restart
```

Restoring Faspex

Steps to take when restoring Faspex from a backup.

As described in the topic *Save/Restore*, you can create a backup file of your Faspex configuration folder and database by going to **Server** > **Configuration** > **Save/Restore** . From this screen, you may also restore your Faspex configuration folder and database on a new machine. In addition to uploading the backup file and selecting the **Restore** button, there are additional steps that need to be followed when restoring Faspex on a new machine.

WARNING! Use caution when restoring your Faspex configuration and database! The restore version (that which you saved) *MUST* match your currently installed version of Faspex.

IMPORTANT NOTE: If you created *post-processing scripts*, you must copy and restore them manually. Faspex does not automatically save them for you.

1. Install your Faspex license file on the new server.

   Copy the license file to the new server. (If this is an On-Demand system, you must rerun the entitlement.) For information on installing a license, or obtaining a new one from Aspera, see *License*.

2. Copy your SSL certificates and keys.

   If you have a custom SSL Certificate, or want to preserve the existing one, copy the SSL certificates and keys to the following locations:

OS Version	File Location
32-bit Windows	`C:\Program Files\Common Files\Aspera\Common\apache\conf\server.crt`
	`C:\Program Files\Common Files\Aspera\Common\apache\conf\server.key`
64-bit Windows	`C:\Program Files(x86)\Common Files\Aspera\Common\apache\conf\server.crt`
	`C:\Program Files(x86)\Common Files\Aspera\Common\apache\conf\server.key`

   Keep a backup of those files in that directory.

3. Reset your Faspex hostname.

To change your Faspex hostname (since it does not get carried over during the backup/restore process), run the following command:

```
> asctl apache:hostname HOSTNAME
```

4. Update *aspera.conf* with the new hostname.

   Open *aspera.conf*, which you can find in the following location:

OS Version	File Location
32-bit Windows	C:\Program Files\Aspera\Enterprise Server\etc\
64-bit Windows	C:\Program Files (x86)\Aspera\Enterprise Server\etc\

   Modify *aspera.conf* to include the new hostname:

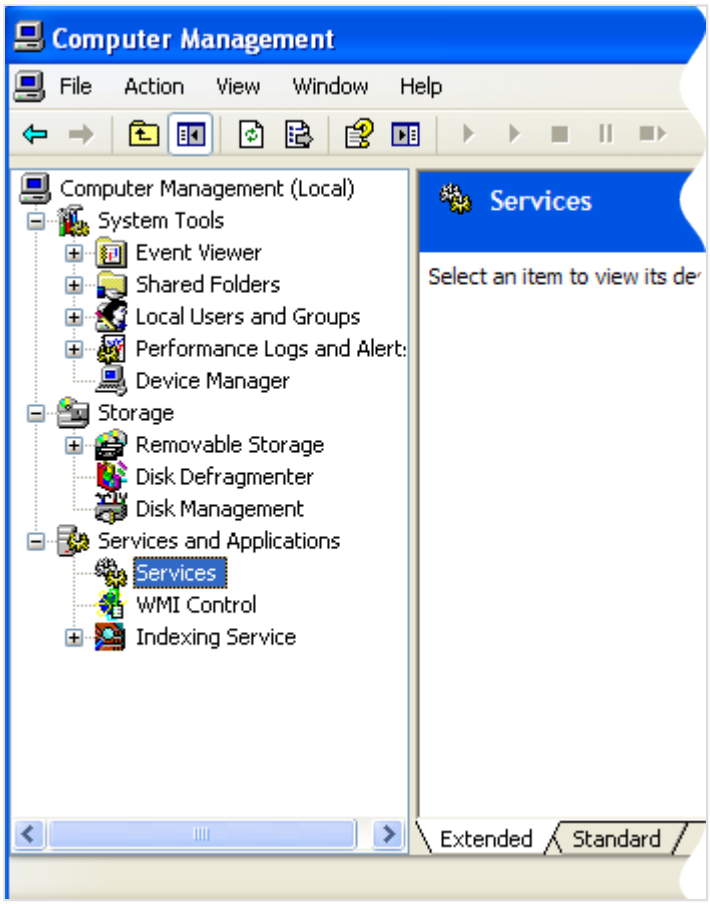
```
...
<server>
    <server_name>HOSTNAME</server_name>
</server>
...
```

5. For Faspex On-Demand systems: Update *aspera.conf* to provide the Faspex user's S3 docroot setting.
6. Restart Aspera services.

   After changing *aspera.conf*, restart the following services:

   - Aspera NodeD
   - Aspera HTTPD
   - Faspex

   You can restart **Aspera NodeD** and **Aspera HTTPD** within the Computer Management window, which is accessible from **Manage** > **Services and Applications** > **Services** .



To restart Faspex, run the following command in a Command Prompt:

```
> asctl faspex:restart
```

7. Migrate the server to the new public IP (or EIP in Amazon if you're using an On-Demand system), or change your DNS to point the hostname to the new server IP.

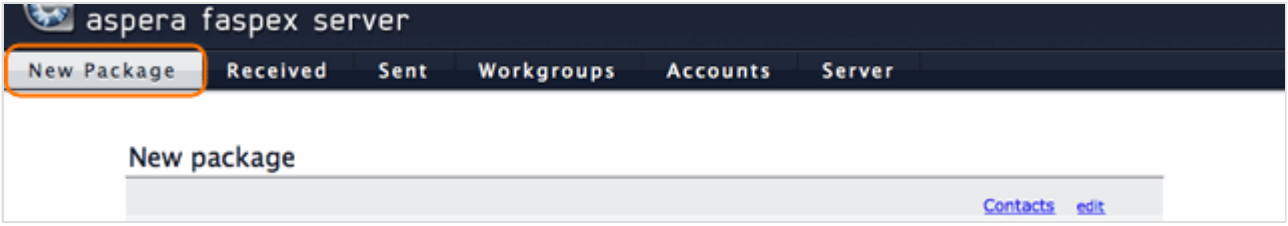
Sending and Receiving Packages

Transfer files with Aspera Faspex packages

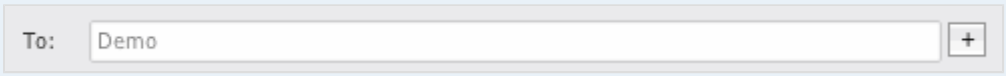
Sending Packages

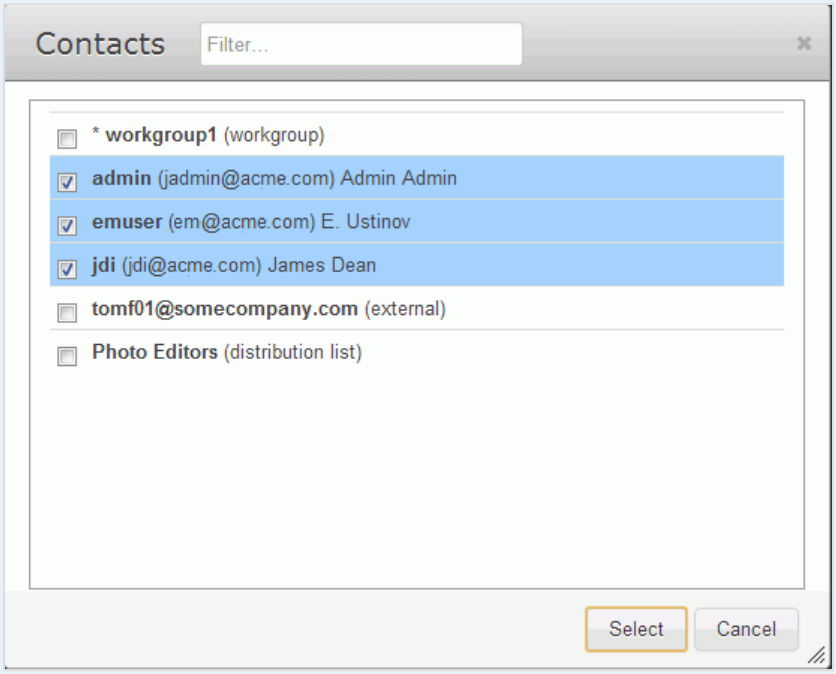
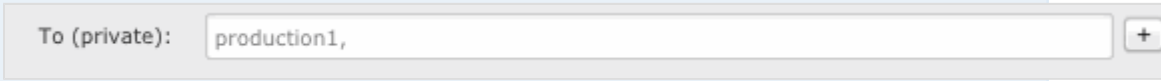
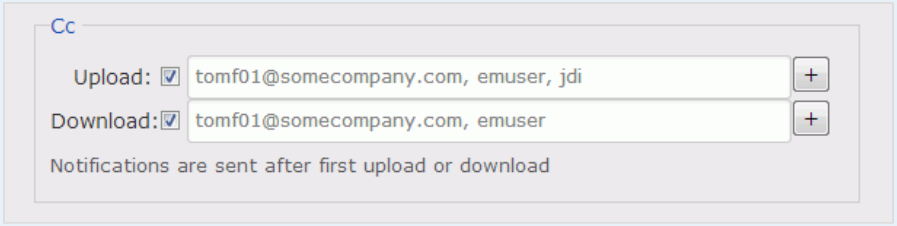
Send file packages using Faspex.

To send file packages, go to **New Package** from the Faspex menu.



Depending on your Faspex server configuration, your *New Package* screen may vary. All potential options in the New Package form are listed below:

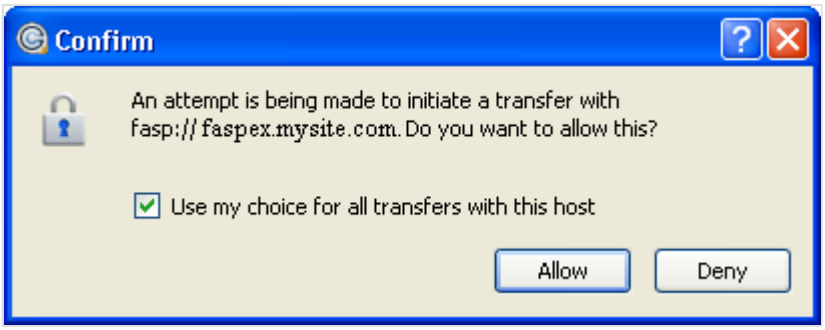
Option	Description
To	Enter the package recipients on the **To** line. A recipient can be a Faspex account name, the email address of an external user (if this is permitted for your account), a workgroup name (workgroup names begin with an asterisk (*)), or a name of a distribution list  To view your contact list, click the  button. In addition to Faspex users, the contact list will show your workgroups and distirbution lists. If you are permitted to send packages to external email addresses, and you have sent files to a new address, Faspex also saves the address into your contact list. To remove it from your list, go to **Accounts** > > **Edit Contacts** (for additional information, see the topic "*Account (Preferences)*").

Option	Description
	
To (private)	You can send a package as a BCC (blind carbon-copy) to other users by entering Faspex account names, external email addresses (if allowed), or distribution lists in this field. To hide this field, click the **Hide Private Recipients** link. 
CC (upload/download)	You can notify others when packages are uploaded and/or downloaded by enabling these fields and entering Faspex account names or email addresses. However, you cannot enter workgroups or distribution lists in this field. To hide this field, click **Hide CC**. You can configure the CC notifications by going to **Server** > **Notifications** . For additional information, please review the "*Notifications*" topic. 
Title	The package title (required).

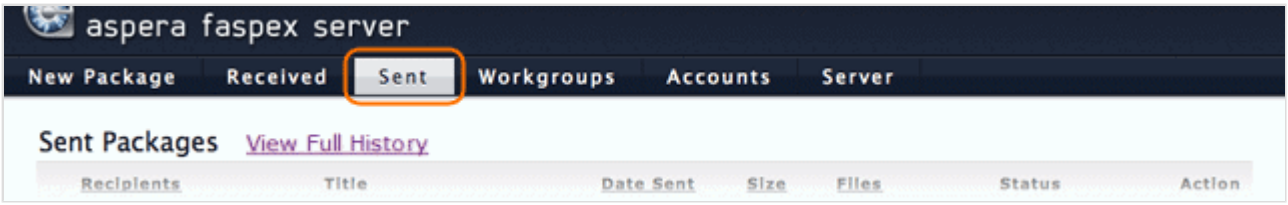
Option	Description
(Custom Metadata)	Faspex allows the administrator to add custom metadata fields in the *New Package* form. The information will be added at the beginning of **Note**. Refer to *Metadata* on page 94 for more information.
Note	Optional comments about the package.
Use encryption-at-rest	If allowed by the system administrator, enable (check) the box if you would like to encrypt the package's contents on the server. Note that the recipient(s) will be required to decrypt the package with a password.
Source	If your Faspex Server is enabled to access content from multiple file servers, then you can select your content source from the drop-down list. For example, you may have the option to select whether a package is created from files on your local computer, from files on another computer, or from cloud-based storage. **IMPORTANT NOTE:** Outside submitters will not be able to create packages from remote sources.
Expiration	If the user is allowed to set package expiration rules, this field will offer three options: • **Do nothing**: Do not auto-delete after the package is downloaded. • **Delete files after any recipient downloads all files**: Delete if all files in the package are downloaded once. • **Delete files after all recipient downloads all files**: Delete if all recipients have downloaded the whole package. **IMPORTANT NOTE:** When a package is marked for deletion after download, any packages pointing that point to the files contained therein will not be accessible once the original package is downloaded. This condition could potentially lead to forwarded package files being inaccessible if they are forwarded before being downloaded by the original recipient. To enable or disable this field, refer to *Security* on page 56, *Package Storage* section.
Contents	Click **Browse** and select files or folders to send. You can also drag-and-drop files onto the graphic. Note that the drag-and-drop graphic and capability is only available for local uploads and will not be available when uploading from a remote source.

IMPORTANT NOTE: All standard fields, except **Note**, are required. Metadata fields may be required, if enabled by the administrator.

When a *local* transfer is initiated, Faspex will prompt Aspera Connect to start a session. Remote transfers (if enabled) will not prompt Connect. When the *Confirm* window appears, click **Allow** to begin.



Depending on your Faspex server's setting, the file package you sent are stored on the server for certain days, or until deleted manually. You can find your sent packages in **Sent** from the Faspex menu.



On the *Sent* page, you can shorten the list by moving packages into the archive. Click the **Archive** button in a row to move the package into the archive. To locate archived packages, click **View Full History**.

NOTE: Only global admins and workgroup admins can archive packages. Regular workgroup members cannot archive packages.

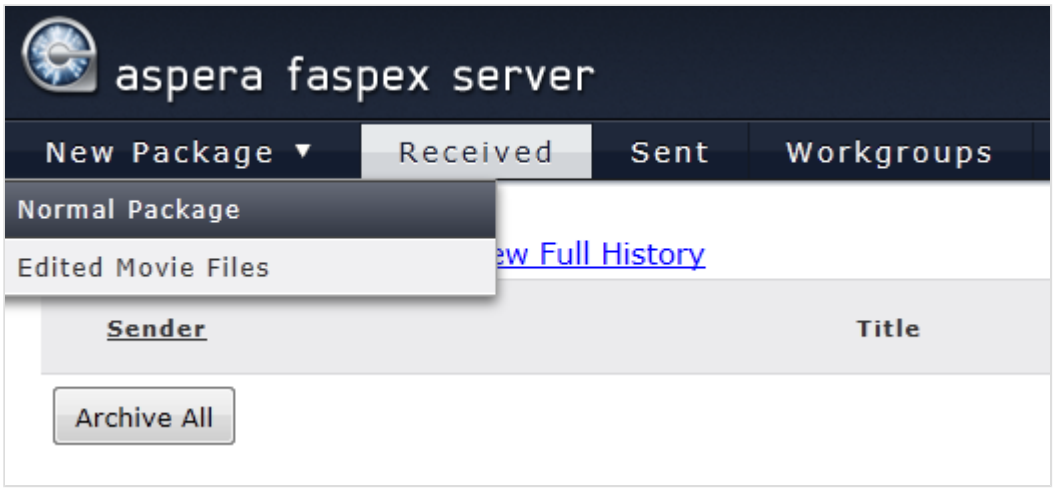
Sending to a Workgroup or Dropbox

Send Packages to a Faspex Workgroup or Dropbox

If you are a Faspex workgroup and/or dropbox member and have been assigned the proper permissions, follow the steps below to send a package to the workgroup and/or dropbox.

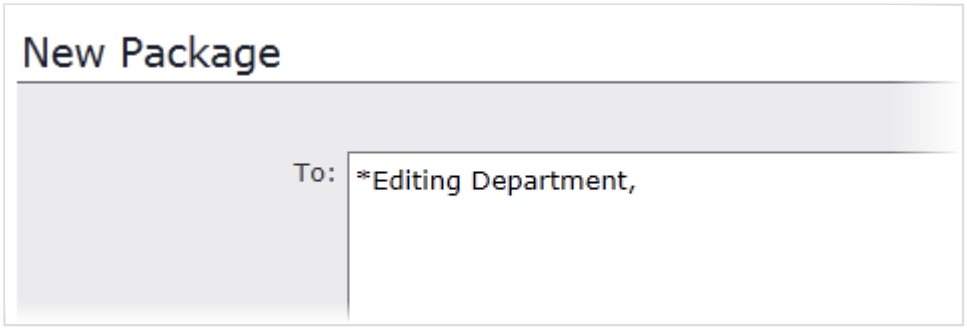
1. Select **New Package** from the Faspex menu.

   - If you are a member of a workgroup *only*, select **New Package** from the Faspex menu.
   - If you are a member of a dropbox or a member of both a workgroup and a dropbox, select **New Package** from the Faspex menu. To send a package to a single Faspex user or workgroup, click **Normal Package**; otherwise, to send to a dropbox, click the name of the dropbox.



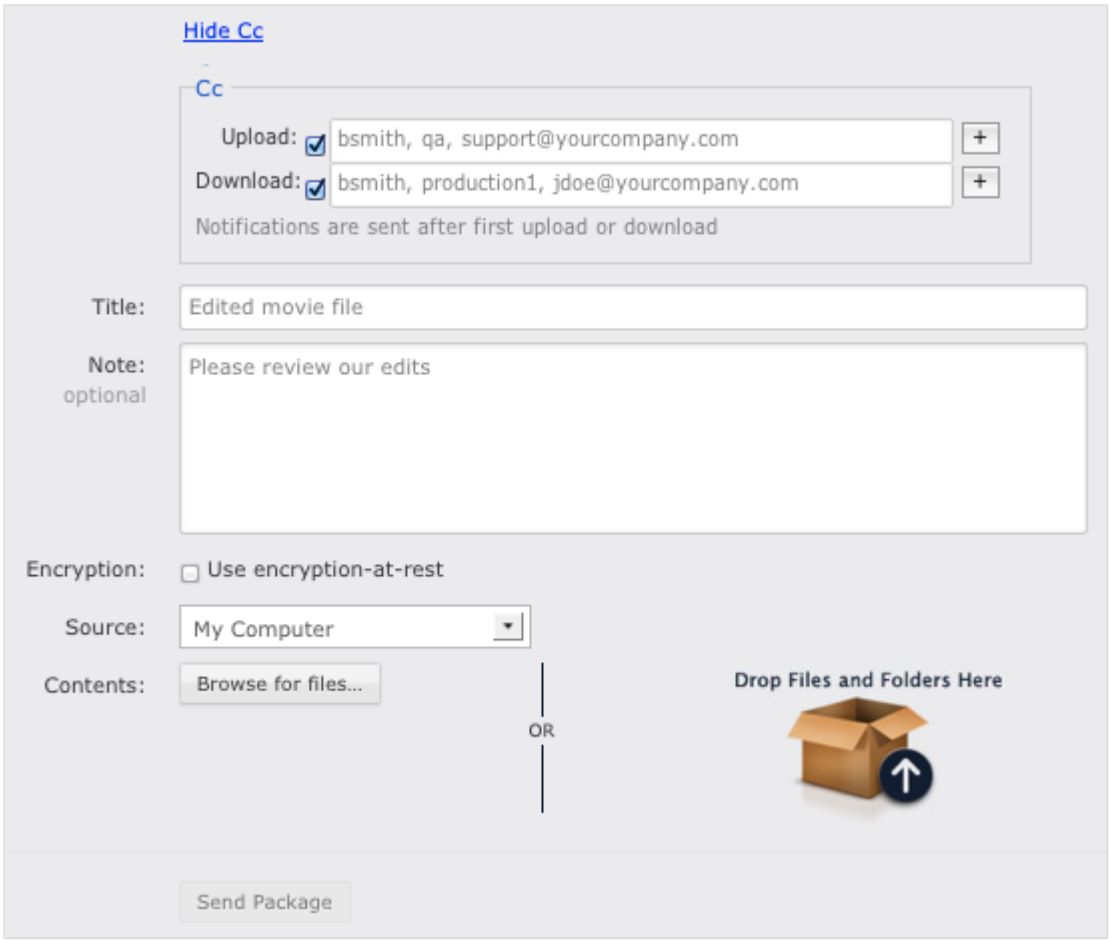
2. *(When sending to Workgroups)* Address the package to designated workgroup and complete the submission form

   Follow the instructions shown in the topic *Sending Packages* on page 146 for completing the *Send Package* form. Input the workgroup's name into the *To:* field. Note that workgroups are preceded by an asterisk (*).



3. *(When sending to Dropboxes)* Complete the submission form

   Follow the instructions shown in the topic *Sending Packages* on page 146 for completing the *Send to Dropbox* form. The *To:* and *To (private):* fields are not displayed since you are sending to a designated dropbox.



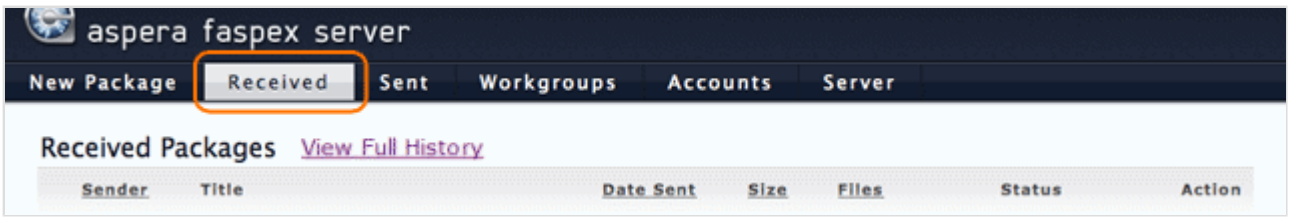
Receiving Packages

Receive file packages from Faspex.

This topic demonstrates how to access Faspex packages that have been sent to your Workgroup, Dropbox or directly to your Faspex account. Note that you can enable the Faspex email notification feature for when you receive a new package. Please refer to *Account (Preferences)* on page 29 for details.

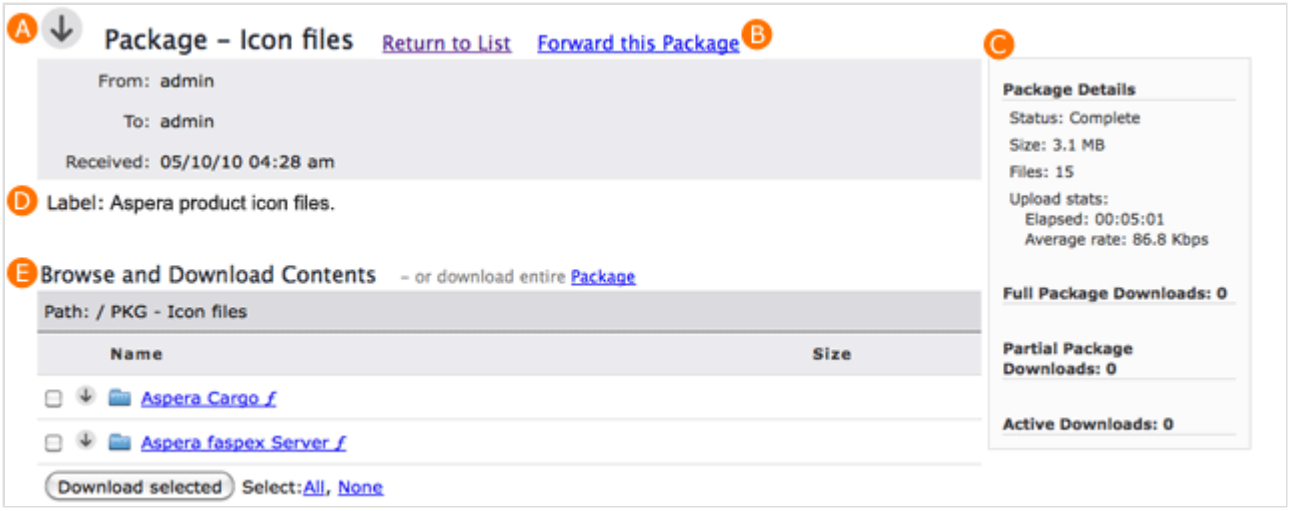
Downloading a package sent directly to your Faspex user account

To download file packages that have been sent directly to you, click **Received** within the Faspex menu.



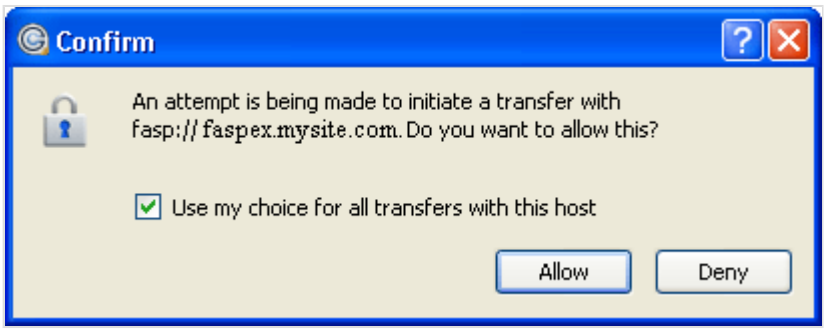
In the received packages list, you can click the header bar links to sort your packages. For example, when clicking *Sender*, all packages are sorted alphabetically by sender's name, or reverse-alphabetically when clicking twice. To

download a package, click the  , or click the package name to advance to its *Details* page. The package detail page contains the following items:



Item	Name	Description
A	Download Icon	Click the icon to download the complete package.
B	Forward this Package	If package forwarding is allowed on your user account, click the link to forward this package.
C	Package Details	The package's information and download activity.
D	Package Note and metadata	The package's note and metadata, if any.
E	Browse and Download Contents	Navigate into folders in this package, or select folders and files to download.

Once you have initiated the download, you will be asked to confirm your download directory; after which, Faspex will prompt Aspera Connect to start a session. When the *Confirm* window appears, click **Allow** to begin.

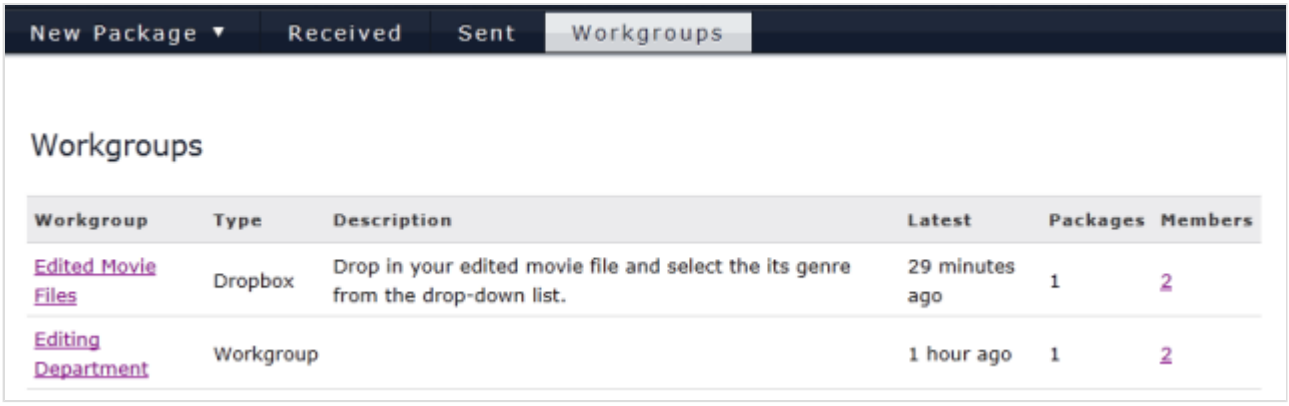


Note that you can shorten your received packages list by moving packages into archive. To do so, click the **Archive** link within the corresponding package row (under the *Actions* column. To locate archived packages, click **View Full History** link.

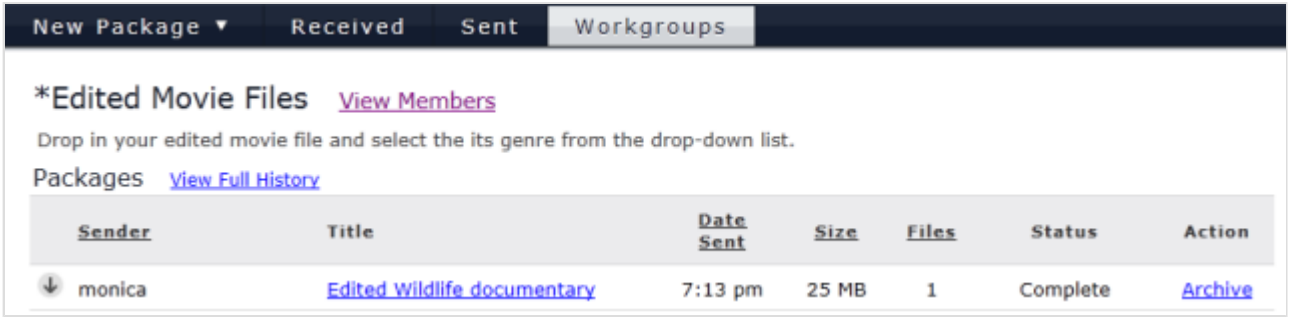
NOTE: Only global admins and workgroup admins can archive packages. Regular workgroup members cannot archive packages.

Downloading a package sent to your Faspex Workgroup or Dropbox

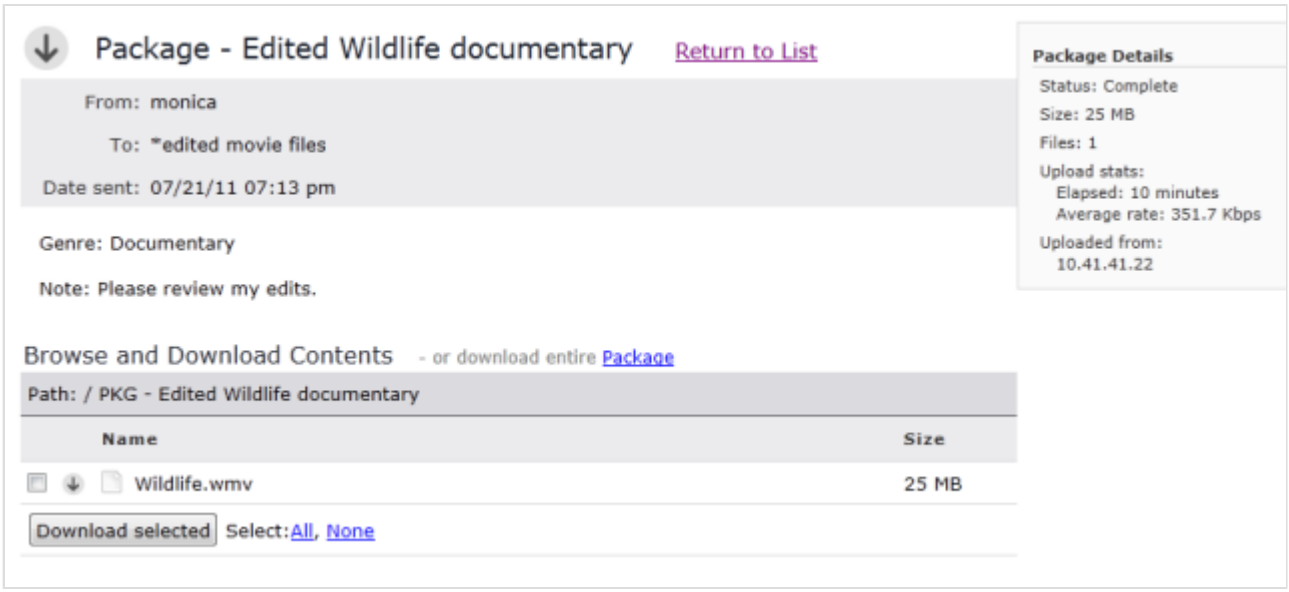
If you are a member of a Faspex Workgroup or Dropbox, you can download file packages that have been sent to your Workgroup or Dropbox from the **Workgroups** tab (in the Faspex menu).



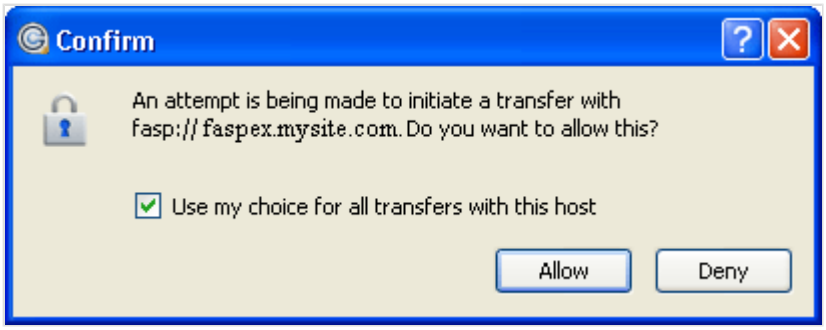
After selecting the **Workgroups** tab--in the received packages list--you can click the header bar links to sort your packages. For example, when *Sender* is clicked, all packages are sorted alphabetically by sender's name (or reverse-alphabetically when clicked twice). To download a package, click the  , or click the package name to advance to its *Details* page.



From the *Details* page, you can either browse and download individual files, or click the **Package** link to download the entire package.

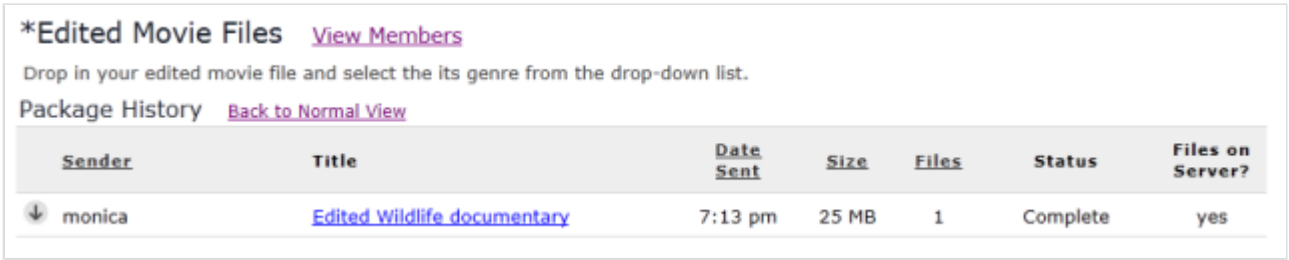


Once you have initiated the download, you will be asked to confirm your download directory; after which, Faspex will prompt Aspera Connect to start a session. When the *Confirm* window appears, click **Allow** to begin.



Note that you can shorten the workgroup's or dropbox's downloaded packages list by moving packages into archive. To do so, click the **Archive** link within the corresponding package row (under the *Actions* column). To locate archived packages, click the **View Full History** link.

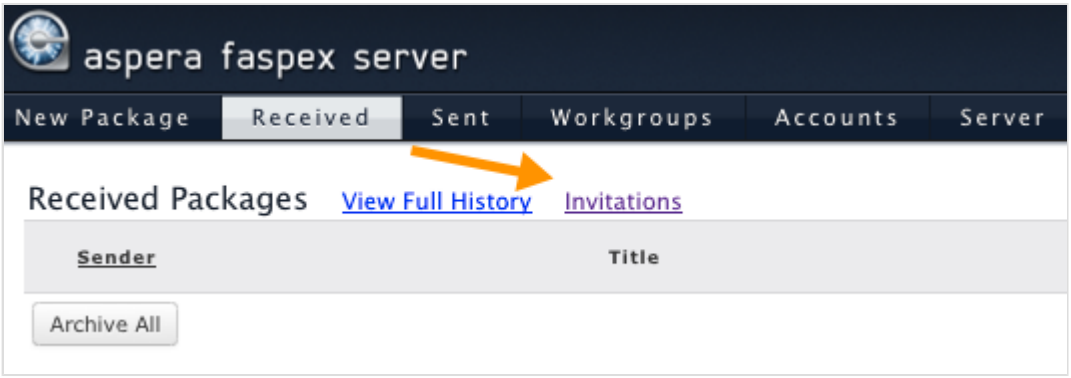
NOTE: Only global admins and workgroup admins can archive packages. Regular workgroup members cannot archive packages.



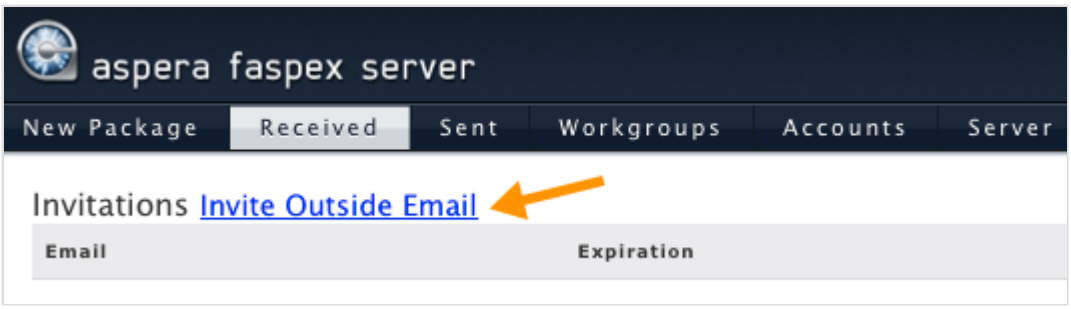
Inviting External Senders

Invite outside users to send a package.

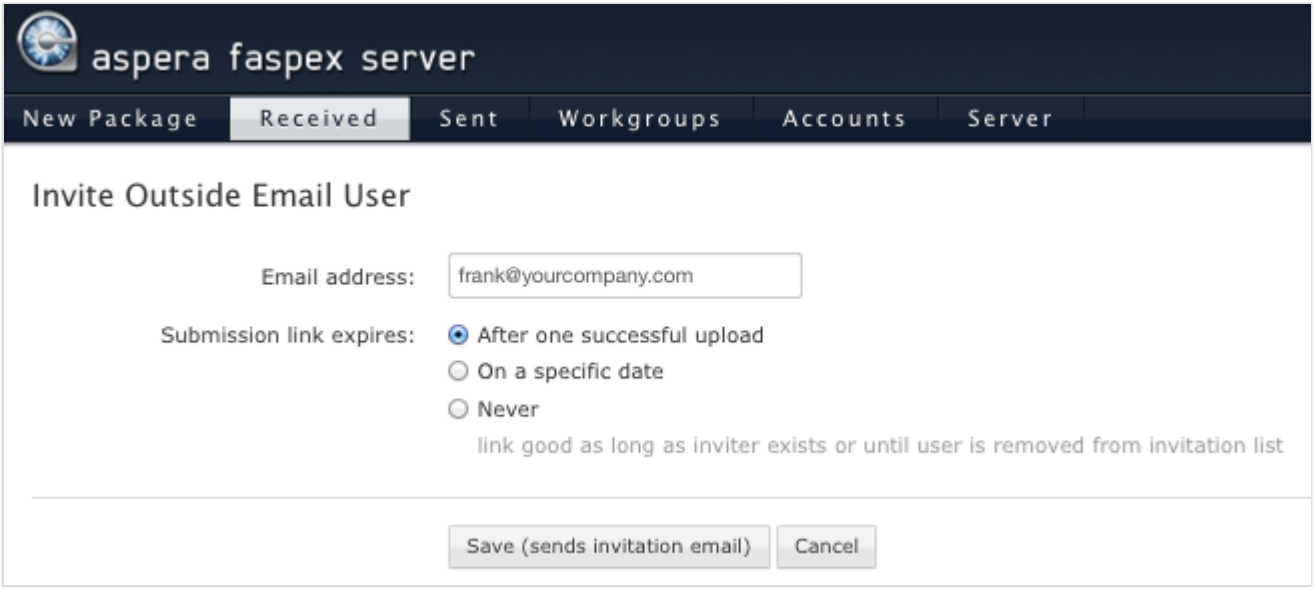
If you have enabled the feature **Allow inviting external senders** under **Server** > **Configuration** > **Security** , then a non-registered user can easily send you a Faspex package. Before continuing, please confirm that this feature is enabled under your *Security* settings. To send an invitation, go to the Faspex **Received** menu and select the **Invitations** link at the top of the page.



On the *Invitations* screen, you will see any invitations that you have already sent, as well as a link to **Invite Outside Email**. Click this link to send an invitation.



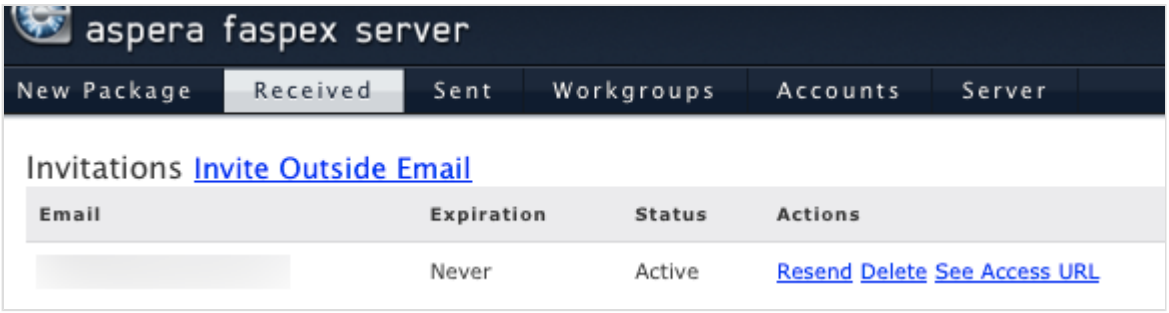
On the following page, you will be required to enter the outside sender's email address, as well as the submission link rules.



The submission link rules include the following:

- Delete the submission link after one successful upload
- Delete the submission link on a specific date (which you will need to input)
- Never delete the submission link as long as the inviter (you) exists or until the sender is removed from the invitation list.

The user will then receive an email from Faspex, along with a submission link, so that he or she can send you a package (i.e. perform an upload). You can view all your invitations by going back to **Received** > **Invitations** .



Here, you can perform the following operations:

- You can resend the submission link.
- You can delete the invitation (which removes the sender from this list and prevents them from using the submission link).
- You can see the URL (submission link) that has been sent to the user.

Appendix

Updating Aspera Service Account

Lookup or change the user account that runs Aspera services.

On Windows, a special user account (Aspera service account) is used to run the services for Aspera products (*Aspera Central, Aspera HTTPD, Aspera Sync, and OpenSSH Service (if selected to install)*). During the installation, you are prompted to create a new Aspera service account, or add an existing user account for this purpose.

This topic covers the configuration of the Aspera service account, including updating the existing Aspera service account's password, and changing the Aspera service account.

1. Update the existing Aspera service account's password

   During the installation, if you are having any problems entering the existing Aspera service account's credentials, change the user's password. To do so, right-click on **My Computer** and select **Manage** > **Local Users and Groups** > **Users**. Right-click on the account name and select **Set Password...**.

2. Change Aspera service account

   Replace the logon user running all Aspera services, open Command Prompt (**Start menu** > **All Programs** > **Accessories** > **Command Prompt**) and use the *asuser-services.bat* command.

   In the Command Prompt, navigate into the path that contains this command:

OS Version	Command
32-bit Windows	`> cd "\Program Files\Aspera\Enterprise Server\bin"`
64-bit Windows	`> cd "\Program Files (x86)\Aspera\Enterprise Server\bin"`

   For example, to use an existing domain user (*asp1@domain.acme.com* / *myPassword*), execute the command:

```
> asuser-services.bat  asp1@domain.acme.com  myPassword
```

   If you are entering a non-existent user account, this command will create the system user. For example, to set up a new user as the Aspera service account:

```
> asuser-services.bat  newUser  newUserPassword
```

If you are running a non-english version of Windows, your administrator group may not be "Administrators". When updating Aspera service account, add a third parameter that specifies the local admin group:

```
> asuser-services.bat  newUser  newUserPassword Administratores
```

Setting up a Remote Server

Steps on setting up a remote transfer-server node for Faspex.

Follow the steps below to set up a remote transfer-server node for Faspex. Note that all steps must be performed on the remote machine (transfer server), as the **Administrator**.

1. Create the system user.

   This is the user who authenticates the actual ascp transfer, and must be an operating system account. To create a new system user "`faspex`" on your Windows system, go to **Control Panel** > **User Accounts** . After adding the `faspex` user, change the user's password.

2. Create and configure the faspex package directory.

   Create the following directory:

   ```
   C:\faspex_packages
   ```

3. Modify aspera.conf.

   Add the faspex package directory as a docroot in `aspera.conf`. The `aspera.conf` file can be found in the following location:

OS Version	File Location
32-bit Windows	`C:\Program Files\Aspera\Enterprise Server\etc\aspera.conf`
64-bit Windows	`C:\Program Files (x86)\Aspera\Enterprise Server\etc\aspera.conf`

   Below is a typical Faspex `aspera.conf` file. Yours may differ, particularly if you have installed other Aspera products. Modify the following, as necessary:

   - In the file below, look for the <absolute> tag to see how the docroot has been defined in this installation, and adjust yours accordingly.
   - Look for the <server_name> tag below, and ensure that SERVER_IP_OR_NAME has been replaced with the name or IP address of your server.

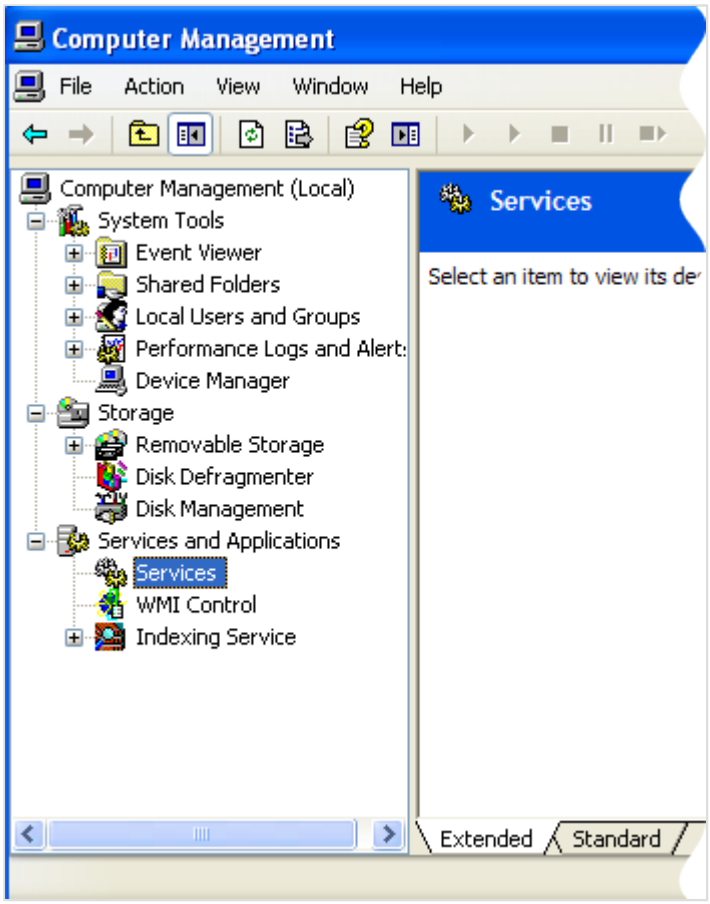
```
<?xml version='1.0' encoding='UTF-8'?>
<CONF version="2">

<central_server>
```

```
  <address>127.0.0.1</address>
  <port>40001</port>
  <compact_on_startup>enable</compact_on_startup>
  <persistent_store>enable</persistent_store>
  <persistent_store_on_error>ignore</persistent_store_on_error>
  <persistent_store_max_age>86400</persistent_store_max_age>
  <event_buffer_overrun>block</event_buffer_overrun>
</central_server>
<default>
  <file_system>
    <pre_calculate_job_size>yes</pre_calculate_job_size>
  </file_system>
</default>
<aaa>
  <realms>
    <realm>
      <users>
        <user>
          <name>faspex</name>
          <file_system>
            <access>
              <paths>
                <path>
                  <absolute>C:\faspex_packages</absolute>
                  <show_as>/</show_as>
                  <dir_allowed>true</dir_allowed>
                </path>
              </paths>
            </access>
            <directory_create_mode>770</directory_create_mode>
            <file_create_mode>660</file_create_mode>
          </file_system>
          <authorization>
            <transfer>
              <in>
                <value>token</value>
              </in>
              <out>
                <value>token</value>
              </out>
            </transfer>
            <token>
```

```
              <encryption_key>af208360-dbdd-4033-a35b-2370941f37e9</encryption_key>
            </token>
          </authorization>
        </user>
      </users>
    </realm>
  </realms>
</aaa>
<http_server>
  <http_port>8080</http_port>
  <enable_http>1</enable_http>
  <https_port>8443</https_port>
  <enable_https>1</enable_https>
</http_server>
<server>
  <server_name>SERVER_IP_OR_NAME</server_name>
</server>
</CONF>
```

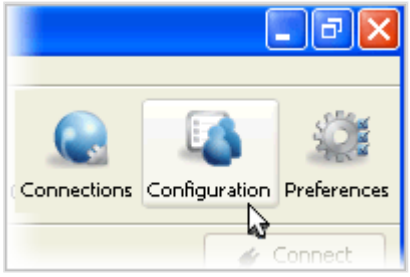
After modifying `aspera.conf`, restart **Aspera Central** and **Aspera NodeD** services.

You can restart these services from the Windows Computer Management window, accessible from **Manage** > **Services and Applications** > **Services** .



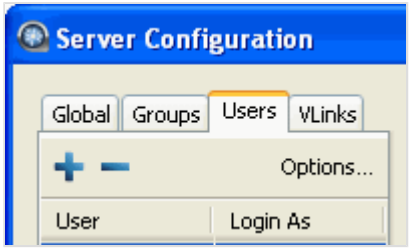
4. Add the faspex user to your Aspera server.

   Launch the application (**Start menu** > **All Programs** > **Aspera** > **Enterprise Server** > **Enterprise Server**) and click **Configuration**.



Click the Configuration.

Within *Server Configuration*, select the **Users** tab and click the  button.



5. Verify your transfer server license.

   Verify that you have installed a valid Faspex license on your transfer server. If you need to update your transfer server license (by following the instructions in your server guide), you must reload the **asperanoded** service afterwards. Reload the asperanoded service by running asnodeadmin.exe, found in the following location:

OS Version	File Location
32-bit Windows	`C:\Program Files\Aspera\Enterprise Server\bin\asnodeadmin.exe`
64-bit Windows	`C:\Program Files (x86)\Aspera\Enterprise Server\bin\asnodeadmin.exe`

```
> asnodeadmin.exe --reload
```

6. Set up the node user.

   Run the following commands to set up the node user (where "`node-admin`" is the node user, "`s3cur3_p433`" is his password and "`faspex`" is the system user), and then reload **asperanoded**.

```
> asnodeadmin.exe -a -u node-admin -p s3cur3_p433 -x faspex
> asnodeadmin.exe --reload
```

7. Install the Connect key.

   First, locate your Connect key as follows:

OS Version	File Location
32-bit Windows	C:\Program Files\Aspera\Enterprise Server\var\aspera_id_dsa.pub
64-bit Windows	C:\Program Files (x86)\Aspera\Enterprise Server\var\aspera_id_dsa.pub

   Then, run the following commands in a terminal window to create a **.ssh** folder (if it does not already exist) in the `faspex` user's home directory:

```
> cd "C:\Documents and Settings\faspex"
> md .ssh
```

   Use a text editor to create (or edit) the following file, without the file extension:

```
C:\Documents and Settings\faspex\.ssh\authorized_keys
```

   Add the `faspex` user's key string into this file and save it. Note that some text editors add a **.txt** extension to the filename automatically. Be sure to remove the extension if it was added to the filename.

8. Configure your remote transfer server in the Faspex Web GUI.

Follow the instructions in the topic "*Transfer Server*" for configuring your remote transfer server in the Faspex Web GUI (**Server** > **File Storage**).

Note on Encryption at Rest

Details about Faspex Server's EAR setting

As described in *Security* on page 56, the **Use Encryption-at-Rest** checkbox setting--*when enabled*--requires users, on upload, to enter a password to encrypt the files on the server. Package recipients will be required to enter the password to decrypt protected files as they are being downloaded. If a user elects to keep downloaded files encrypted, then they do not need to enter a password until they attempt to decrypt the files locally. Encryption-at-Rest is supported by the Aspera Connect Browser Plug-in, starting with Version 2.2.0. To ensure that encryption and decryption occur, log in to your Faspex Server GUI, select **Server** > **Configuration** > **Transfers** and scroll down to the *Aspera Connect Version* section. Please mark the **Enforce minimum version** checkbox and specify "2.2.0" or higher in the **Version** field.

IMPORTANT NOTE: The *Use Encryption-at-Rest* feature is not fully enforced unless the Faspex Server Administrator also updates the *aspera.conf* configuration file (which is not automatically modified by Faspex). The Administrator may update *aspera.conf* manually or through the Enterprise Server GUI (please refer to *http://www.asperasoft.com/en/documentation/1* for details on the GUI). Within *aspera.conf*, the **Content Protection Required** and **Content Protection Strong Password Required** must be enabled.

The following code block demonstrates manually updating *aspera.conf*:

```
<transfer>
...
 <encryption>
    <content_protection_strong_pass_required>  <!--Strong Password Required for
 Content Protection-->
       true
    </content_protection_strong_pass_required>
    <content_protection_required>              <!--Content Protection Required-->
       true
    </content_protection_required>
 ...
 </encryption>
...
</transfer>
```

IMPORTANT NOTE on using HTTP Fallback with Faspex Server

The Aspera HTTP Fallback Server provides a secondary transfer method for clients that don't have the Internet connectivity required for Aspera accelerated transfers (By default, UDP port 33001). When UDP connectivity is lost or cannot be established, the transfer will be continued over the HTTP protocol. If transfer encryption is enabled, the transfer will continue over HTTPS. For details on configuring HTTP Fallback for Faspex Server, please refer to *Configuring HTTP and HTTPS Fallback* on page 138

When a transfer falls back to HTTP or HTTPS, ***content protection is no longer supported***. If HTTP fallback occurs while *downloading*, then--despite entering a passphrase--the files will remain encrypted (i.e., enveloped). If HTTP fallback occurs while *uploading*, then--despite entering a passphrase--the files will NOT be encrypted (i.e., enveloped).

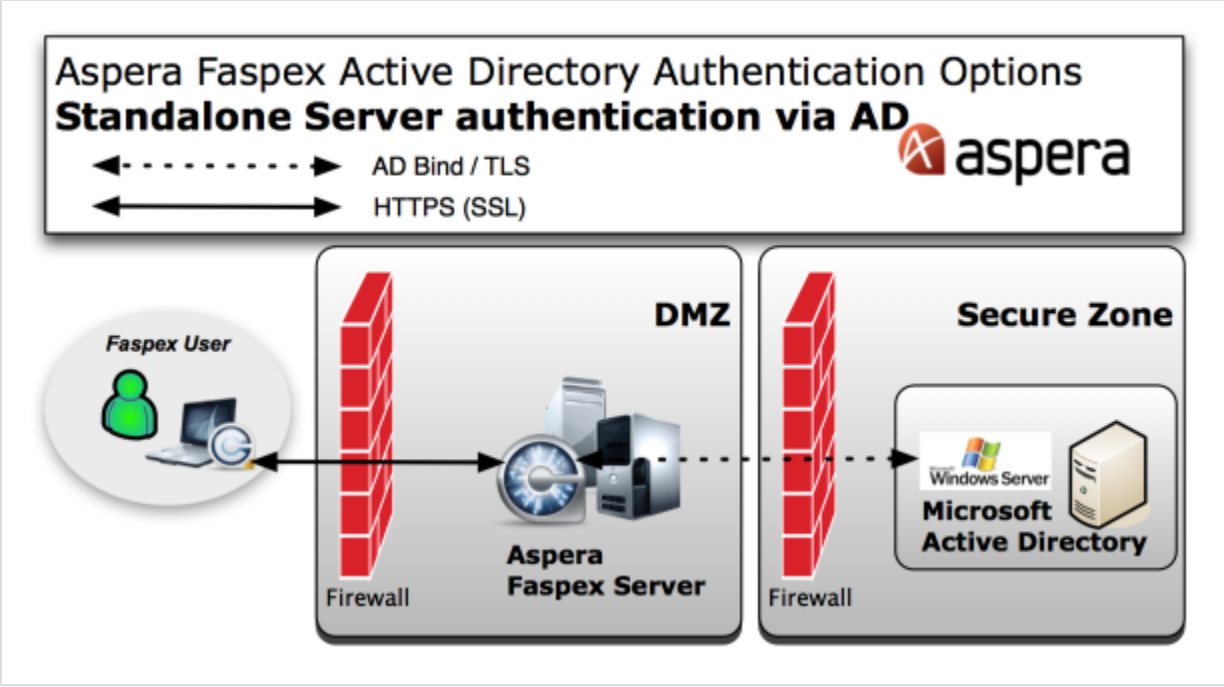
User Authentication Options with AD

Deployment scenarios for Faspex Server with Active Directory (AD) user authentication

This topic describes different deployment scenarios for Aspera Faspex Server with Active Directory (AD) user authentication.

Scenario 1: Standalone Faspex Server Authentication via AD

You must first configure the standalone Faspex Server to bind to the Active Directory. To do so, please refer to the instructions in the topic *Authentication: Directory Service* on page 77. The figure below depicts this scenario's information workflow.



Please review the following important notes for the standalone scenario:

- It is **not necessary** for the Faspex Server to join the Windows domain.

- The bind may use a read-only AD account.
- Some organizations deploy read-only (proxy) instances of their AD in the DMZ for a higher level of security.
- Some organization deploy dedicated security servers, such as Microsoft ISA to secure the bind from the DMZ to the secure zone.

NOTE ON TLS: As of Faspex Server version 2.0.5+, the ability to query AD services via TLS (i.e. a secure connection) is now supported. As a result, it is feasible to establish the AD bind over an unsecure network.

asctl Command Reference

Use asctl commands to control *Faspex*-related services.

You can utilize the asctl commands in a **Command window** to display or modify *Faspex Server's* component settings. This topic lists all *Faspex Server* configuration options that can be modified using asctl. If there are modifications that cannot be accomplished with asctl, please notify Aspera Support.

Component	Description
Directory Service (DS)	Faspex's Directory Service support.
Apache	Apache web server.
Background	Process new data from the MySQL database.
Faspex	Faspex main application.
Mongrel	Ruby's HTTP library.
MySQL	MySQL database.

All components commands

IMPORTANT NOTE: The commands in this section control all *Faspex Server* components.

Task	Command	Description
Show config info	asctl all:info	Print info about all components.
Restart all components	asctl all:restart	Restart all components.
Setup status	asctl all:setup_status	Information about configuring all components.
Start	asctl all:start	Start all components.

Task	Command	Description
Show status	asctl all:status	Display the status of each component.
Stop	asctl all:stop	Stop all components.
Show version	asctl all:version	Display the current version of each component.

Directory Service (DS)

Task	Command	Additional information
Start DS	asctl faspex:ds:start	
Stop DS	asctl faspex:ds:stop	
Restart DS	asctl faspex:ds:restart	
Show DS status	asctl faspex:ds:status	
Disable DS	asctl faspex:ds:disable	When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.

Apache

Task	Command	Additional Information
Create a setup file	asctl apache:create_setup_file <file>	Create a reusable file that contains answers to the setup questions. Replace <file> with a file name.
(Deprecated) Clean up Apache logs	asctl apache:delete_logs_older_than <X>_days **IMPORTANT NOTE:** This command has been deprecated for *Faspex Server version 2.0.7+*. For *Faspex Server version 2.0.7+*, all Apache logs are, by default, rotated by size (defaulting to 10Mb files and only retaining the last 10 rotated logs).	Delete log files older than the specified number of days. Replace <X> with a number.

Task	Command	Additional Information
Disable Apache	asctl apache:disable	Disable Aspera's Apache. When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.
Disable Apache logs	asctl apache:disable_logs	Set the Apache's log level to 'emerg'.
Enable Apache logs	asctl apache:enable_logs	Set the Apache's log level to 'notice'.
Re-generate conf	asctl apache:generate_config	Generate Faspex Server component's configuration file using the current settings.
Display hostname	asctl apache:hostname	Display the hostname or IP address of the server.
Change hostname	asctl apache:hostname <host>	Change the hostname or IP address of the server. Replace <host> with a new hostname or IP address.
Display HTTP port	asctl apache:http_port	Display the HTTP port the web server listens to.
Change HTTP port	asctl apache:http_port <port>	Change the HTTP port the web server listens to. Replace <port> with a new port number.
Display HTTPS port	asctl apache:https_port	Display the HTTPS port the web server listens to.
Change HTTPS port	asctl apache:https_port <port>	Change the HTTPS port the web server listens to. Replace <port> with a new port number.
Show config info	asctl apache:info	Print configuration info about Apache.
Copy your SSL files into Aspera's default location (under default names)	asctl apache:install_ssl_cert cert_file key_file [chain_file]	After upgrading Faspex and Common, use this command to copy your original SSL certificate, key and optional chain file to `/opt/aspera/common/apache/conf` and give them Aspera-standard names. The `httpd-ssl.conf` file

Task	Command	Additional Information
		is also re-rendered and permissions/ ownership is set for the cert files.
Set Apache log level	asctl apache:log_level <option>	Specify the Apache's log level. Replace option with **crit**, **error**, **warn**, **notice**, **info** or **debug**.
Create SSL certificate	asctl apache:make_ssl_cert <host>	Create a self-signed SSL certificate for the specified hostname. Replace <host> with your hostname.
Restart Apache	asctl apache:restart	
Configure Apache	asctl apache:setup	
Configure Apache using saved file	asctl apache:setup_from_file <file>	Run setup using the answers from a file created using the "create_setup_file" command.
Start Apache	asctl apache:start	
Show Apache status	asctl apache:status	
Stop Apache	asctl apache:stop	
Upgrade Apache	asctl apache:upgrade	
Show Apache's version	asctl apache:version	

Background

Task	Command	Additional Information
Start Faspex background service	asctl faspex:background:start	
Stop Faspex background service	asctl faspex:background:stop	
Restart Faspex background service	asctl faspex:background:restart	
Show Faspex background service status	asctl faspex:background:status	
Disable Faspex background service	asctl faspex:background:disable	When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.

Faspex Database (DB) Background

Task	Command	Additional Information
Start Faspex DB background service	asctl faspex:db:start	
Stop Faspex DB background service	asctl faspex:db:stop	
Restart Faspex DB background service	asctl faspex:db:restart	
Show Faspex DB background service status	asctl faspex:db:status	

Faspex Node Poller (NP) Background

Task	Command	Additional Information
Start Faspex NP background service	asctl faspex:np:start	
Stop Faspex NP background service	asctl faspex:np:stop	
Restart Faspex NP background service	asctl faspex:np:restart	
Show Faspex NP background service status	asctl faspex:np:status	

Faspex

Task	Command	Description
Setup	asctl faspex:setup	Set up Faspex.
Setup status	asctl faspex:setup_status	Information about configuring this component.
Re-generate conf	asctl faspex:generate_config	Generate Faspex configuration file using the current settings.
Show package dir	asctl faspex:package_dir	Show current directory that Faspex uses to store packages.
Change package dir	asctl faspex:package_dir <dir>	Change directory that Faspex uses to store packages. Replace <dir> with the new path.
Upgrade	asctl faspex:upgrade	Upgrade Faspex from a previous version.
Show config info	asctl faspex:info	Print configuration info about Faspex.

Task	Command	Description
Display URI namespace	asctl faspex:uri_namespace	Display the URI namespace.
Change URI namespace	asctl faspex:uri_namespace <namespace>	Change the URI namespace. Replace <namespace> with a new namespace.
Display mongrel number	asctl faspex:mongrel_count	Display the number of ports the web server listens to.
Change mongrel number	asctl faspex:mongrel_count <number>	Change the number of ports the web server listens to. Replace <number> with a number.
Display lowest mongrel port number	asctl faspex:base_port	Display the lowest port for the mongrel instances.
Change lowest mongrel port number	asctl faspex:base_port <number>	Change the lowest port for the mongrel instances. Replace <number> with a number.
Display HTTP Fallback port	asctl faspex:http_fallback_port	Display the port for HTTP Fallback.
Change HTTP Fallback port	asctl faspex:http_fallback_port <port>	Change the port for HTTP Fallback. Replace <port> with a new port number.
Backup Faspex database	asctl faspex:backup_databases	Backup Faspex database and save the backup files to the path *C:\Program Files\Aspera\Faspex\db\backup*. Refer to *Backing up Faspex Server* for more info.
Migrate Faspex database	asctl faspex:migrate_database	Migrate Faspex MySQL database.
Restore Faspex database	asctl faspex:restore_database	Restore Faspex MySQL database. To restore database, backup files must use default name (central.sql, faspex.sql and user_service.sql).
Create or update admin	asctl faspex:admin_user login email [password]	Create a new admin, or update an existing admin account. Replace login with a login, email with its email. You can add the account's password in the command ([password]), or enter it when

Task	Command	Description
		prompted. If the login you have entered exists, the account is updated with new email and password.
Create setup file	asctl faspex:create_setup_file <file>	Create a reusable file that contains answers to the setup questions. Replace <file> with a file name.
Setup from file	asctl faspex:setup_from_file <file>	Run setup using the answers from a file created using "create_setup_files". Replace <file> with a file name.
Rake command	asctl faspex:rake <arg>	Evoke a rake command.
Show set up version	asctl faspex:version	Display the currently set up version.
Start Faspex	asctl faspex:start	Start Faspex application.
Stop Faspex	asctl faspex:stop	Stop Faspex application.
Restart Faspex	asctl faspex:restart	Restart Faspex application.
Show Faspex status	asctl faspex:status	Display Faspex application's status.
Disable Faspex	asctl faspex:disable	Disable Faspex application. When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.

Mongrel

Task	Command	Description
Start mongrel service	asctl faspex:mongrel:start	Start Faspex's mongrel service.
Stop mongrel service	asctl faspex:mongrel:stop	Stop Faspex's mongrel service.
Restart mongrel	asctl faspex:mongrel:restart	Restart Faspex's mongrel service.
Show mongrel status	asctl faspex:mongrel:status	Display Faspex's mongrel service status.
Disable mongrel	asctl faspex:mongrel:disable	Disable Faspex's mongrel service. When disabled, the service will not start when rebooting computer, does

Task	Command	Description
		not print reminders or update its configurations.

MySQL

Task	Command	Description
Create setup file	asctl mysql:create_setup_file <file>	Create a reusable file that contains answers to the setup questions. Replace <file> with a file name.
Display database directory	asctl mysql:data_dir	Display the directory that the databases are kept in.
Disable MySQL	asctl mysql:disable	Disable Aspera's MySQL. When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.
Grant access on MySQL-only server	asctl mysql:grant_remote_access <host> <mysql_user> <password>	If MySQL server is running on a different computer, use this command on the MySQL machine to allow access from the specified machine. Replace <host>, <mysql_user> and <mysql_password> with the server's hostname, MySQL's user name, and the user's password, respectively.
Show config info	asctl mysql:info	Print configuration info about MySQL.
Show port	asctl mysql:port	Display the port the MySQL server listens to.
Change port	asctl mysql:port <port>	Change the port the MySQL server listens to. Replace <port> with a new port number.
Restart MySQL	asctl mysql:restart	Restart Aspera's MySQL.
Set root password	asctl mysql:set_root_password	Set the password for 'root' in MySQL.

Task	Command	Description
Configure MySQL-only server	asctl mysql:setup	If MySQL server is running on a different computer, use this command on the MySQL machine to configure it.
Configure MySQL using saved file	asctl mysql:setup_from_file <file>	Run setup using the answers from a file created using the "create_setup_file" command.
Start MySQL	asctl mysql:start	Start Aspera's MySQL.
Show MySQL status	asctl mysql:status	Display Aspera's MySQL status.
Stop MySQL	asctl mysql:stop	Stop Aspera's MySQL.
Upgrade MySQL-only server	asctl mysql:upgrade	If MySQL server is running on a different computer, use this command on the MySQL machine to upgrade the database.
Show MySQL's version	asctl mysql:version	Display the currently set up version.

Uninstall

Uninstall Faspex and Enterprise Server from your computer.

Faspex Server consists of both the Faspex Web application and Enterprise Server. This topic shows you how to uninstall both.

1. Uninstall Faspex

   Prior to removing the application, close the following applications and services:

   - Apache HTTPD Server (Aspera)
   - Aspera Central
   - Aspera Faspex Background
   - Aspera Faspex DB Background
   - Aspera Faspex DS Background
   - Aspera Faspex Mongrel
   - Aspera Faspex NP Background
   - Aspera NodeD
   - MySQL Server (Aspera)

You can then uninstall the Faspex Server application via your Windows Control Panel. Depending on your version of Windows, choose **Add/Remove Programs** or **Uninstall a Program**, and select **Aspera Faspex** for removal.

2. Uninstall Enterprise Server

   Prior to removing the application, close the following applications and services:

   - ascp connections
   - SSH connections
   - User interface
   - asperasync Services

   You can then uninstall the Enterprise Server application via your Windows Control Panel. Depending on your version of Windows, choose **Add/Remove Programs** or **Uninstall a Program**, and select **Aspera Enterprise Server** for removal.

Technical Support

For further assistance, you may contact us through the following methods:

Contact Info	
Email	support@asperasoft.com
Phone	+1 (510) 849-2386
Request Form	*http://support.asperasoft.com/home*

The technical support service hours:

Support Type	Hour (Pacific Standard Time, GMT-8)
Standard	8:00am – 6:00pm
Premium	8:00am – 12:00am

We are closed on the following days:

Support Unavailable Dates	
Weekends	Saturday, Sunday
Aspera Holidays	Please refer to our *Website*.

Feedback

The Aspera Technical Publications department wants to hear from you on how Aspera's user manuals can be improved. To submit feedback about this manual, or any other Aspera product document, please visit the *Aspera Product Documentation Feedback Forum*.

Through this forum, you can let us know if you find content that isn't clear or appears incorrect. We also invite you to submit ideas for new topics, as well as ways that we can improve the documentation to make it easier for you to read and implement. When visiting the Aspera Product Documentation Feedback Forum, please remember the following:

- You must be registered to use the Aspera Support Website at *https://support.asperasoft.com/*.
- Be sure to read the forum guidelines before submitting a request.

Legal Notice